AFRL-RI-RS-TR-2009-78
Final Technical Report
March 2009

ROBUST RESOURCE ALLOCATION IN AN AIR OPERATION MODEL AND ROBUST TASKING OF WIRELESS AIRBORNE NETWORKS

State University of New York at Binghamton

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2009-78 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/ /s/

TIMOTHY E. BUSCH
Work Unit Manager

ROBERT S. MCHALE
Deputy Chief, Information Systems Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAR 09	Final	Jun 08 – Sep 08

4. TITLE AND SUBTITLE

ROBUST RESOURCE ALLOCATION IN AN AIR OPERATION MODEL AND ROBUST TASKING OF WIRELESS AIRBORNE NETWORKS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8750-08-1-0223

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)

N. Eva Wu, Xiaohua Edward Li, and Matthew Ruschmann

5d. PROJECT NUMBER
230S

5e. TASK NUMBER
RT

5f. WORK UNIT NUMBER
WA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Research Foundation of the State University of New York at Binghamton
Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RISB
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2009-78

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 88ABW-2009-1131

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The focus of our effort is to study issues regarding robust resource allocation in air operations and robust tasking in wireless airborne networks. For the robust resource allocation, model uncertainties are considered in the generation of a state-based control policy at the strategic level in an air operation. A generic model is used to explain the aspects of modeling, control design, and implementation. Uncertainties are introduced into the transition-rates of the strategic model. A robust and constrained bilinear control problem defined on a probability simplex is solved approximately using a receding horizon control scheme. To achieve robust tasking of wireless airborne networks, we have set up a multiple objective cross-layer optimization framework to compare various multi-hop clustered cooperative transmission schemes. Within this framework, parameters such as cluster size, transmission power and hop patterns can be optimized to enhance signal-to-noise plus interference ratio (SINR), transmission throughput and anti-jamming capability, under the constraint on ISR coverage and network reliability. Our analysis and simulation results indicate that the optimization is in favor of smaller cluster size and shorter transmission distance.

15. SUBJECT TERMS
Robust resource allocation, Robust tasking, Planning, Scheduling, Multi-objective optimization

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Timothy E. Busch
U	U	U	UU	47	19b. TELEPHONE NUMBER (*Include area code*) N/A

Abstract

This report describes the research results under the AFRL grant FA8750-08-1-0223. During the first summer (2008) of the intended three-year project, the focus of our effort is to study issues regarding robust resource allocation in air operations robust tasking in wireless airborne networks.

For the robust resource allocation, model uncertainties are considered in the generation of a state-based control policy at the strategic level in an air operation. A generic model is used to explain the aspects of modeling, control design, and implementation. Uncertainties are introduced into the transition-rates of the strategic model. A robust and constrained bilinear control problem defined on a probability simplex is solved approximately using a receding horizon control scheme. Results obtain previously are show to be robust to uncertainties in the opposing forces abilities.

For robust tasking of wireless airborne networks, we establish a framework suitable for the design of tasking policies for clustered cooperative activities in a dynamic uncertain environment. Since secure and reliable communication is essential in this setting, tasking is confined to that relevant to clustered cooperative communications. In particular, we have set up a multiple objective cross-layer optimization framework to compare various multi-hop clustered cooperative transmission schemes. Within this framework, parameters such as cluster size, transmission power and hop patterns can be optimized to enhance signal-to-noise plus interference ratio (SINR), transmission throughput and anti-jamming capability, under the constraint on ISR coverage and network reliability.

Our analysis and simulation results indicate that the optimization is in favor of smaller cluster size and shorter transmission distance. This complements the outcome of network reliability optimization which is in favor of larger cluster size and with longer transmission distance under the assumption of low channel failure probabilities. Such early results show that robust tasking of wireless airborne networks is a problem well deserving further investigation.

Table of Contents

1. Robust resource allocation in an air operation model 1
1.1 Introduction 1
1.2 Modeling for Control 2
1.2.1 Stochastic Model of Air Operation 2
1.2.2 Bilinear and Input Constrained Design Model 4
1.2.3 Modeling Uncertainty 5
1.3 Control of Strategic Operation 6
1.3.1 Modeling for Dynamic Programming 6
1.3.2 Cost Structure 8
1.3.3 Solution of Min-Max Optimization 8
1.3.4 Closed-Loop Control with SimEvents Model in the Loop 8
1.3.5 Results 10
2. Robust Tasking of Wireless Airborne Networks 12
2.1 Single-link transmission models 13
2.1.1 A clustered secure transmission scheme 14
2.1.2. Clustered beamforming transmission scheme 16
2.1.3 Miscellaneous issues regarding security and reliability 19
2.2 Multi-hop transmission models 22
2.2.1 Transmission and receiving powers and security measure 22
2.2.2 The application of our secure transmission scheme in multi-hop transmission 25
2.2.3 The application of beamforming scheme in multi-hop transmissions 27
2.2.5 Channel failure probability 30
2.3 A numerical example 30
2.3.1 Non-clustered multi-hop relaying 31
2.3.2 Multi-hop relaying with clustered beamforming 33
2.3.3 Multi-hop relaying with clustered secure transmission 34
2.3.4 Network reliability 36
3. Conclusions 38
4. References 39

List of Figures

Figure 1 Concept of control to win on a probability simplex. 1
Figure 2 A low resolution strategic model. 2
Figure 3 An execution of Algorithm 1. Both $t+\tau_{l,q}$ and $t+\tau_{l,n}$ result in a state transition before the next control update. However, the event associated with $t+\tau_{l,n}$ occurs first. 9
Figure 4 The optimal, open-loop control trajectory solved under nominal parameters of the air operation. 10
Figure 5 The optimal, open-loop probability trajectory solved under nominal parameters of the air operation. 10
Figure 6 The optimal, open-loop probability trajectory solved with uncertain transition rates in the air operation. 11
Figure 7 The optimal, open-loop control trajectory solved with uncertain transition rates in the air operation. 11
Figure 8 With a new clustered cooperative secure transmission scheme, Alice can transmit signals to Bob securely against eavesdropper Eve. 13
Figure 9 Illustration of beamforming transmission scheme where a clustered distributed transmission node forms a virtual transmit antenna array. 16
Figure 10 Illustration of real transmission/receiving power and baseband transmission/receiving power model. 22
Figure 11 Multi-hop transmission/receiving powers compared to direct single-hop transmission/receiving powers. 23
Figure 12 Optimization for multi-hop wireless transmission network with non-clustered transmissions. 32
Figure 13 Optimization for multi-hop wireless transmission network with beamforming. 33
Figure 14 Optimization for multi-hop wireless transmission network with clustered secure transmissions 36
Figure 15 Network reliability as a function of time with cluster number as a parameter (Weibull node failure probability assumed, and minimum of 4 surviving agents required for an operative cluster) 37

List of Tables

Table 1 Numerical values (in hours) for transition rates in Fig. 2. 3

Table 2 Non-zero off-diagonal entries of transition rate matrix **Q** 4

Table 3 Steady-state effects of Blue's aggressiveness with different amounts of resources. 4

Table 4 Probabilities of Victory Under Nominal Parameters and Closed- 12

1. Robust resource allocation in an air operation model

1.1 Introduction

When planning a strategic air operation involving two opposing forces (Blue and Red), the model is often viewed as an open-loop process implied by its name [4]. In previous work, [19], an entire military air operation is encompassed into a two-level, two-timescale system. In [20], sub-optimal open-loop and closed-loop control policies are found assuming exact knowledge of the underlying air-operation model. However, model inaccuracies exist due to inaccurate or unavailable knowledge of the operations dynamics. Often little data regarding the opposing force is available. In this paper model inaccuracies are accounted for, and robust control policies are solved.

As in previous work [19, 20], a discrete state variable at the strategic operation level takes the form of the composition of four binary variables (Blue threatened, Blue defeated, Red threatened, and Red defeated). Despite the small number of strategic states, separating the slower strategic process resolves the stiffness problem caused by differing timescales of a strategic operation and a tactical operation. As a result, the faster tactical process can be modeled with greater accuracy, where the state variables take the more conventional forms of asset location, asset strength, their rates of change, etc. In this framework, the strategic state variable enters a tactical operation model as a symbolic parameter, whereas the dynamic effects of the tactical operation are represented by a set of transition coverage parameters that affect the state transition rates in the strategic model.

A bilinear system in a probability simplex naturally results from the strategic model. Between the two absorbing states representing Blue's win and Red's win, respectively, the control objective is to drive the state trajectory to the highest probability that Blue wins, as illustrated in Fig. 1. Uncertainties are introduced into the rates surrounding the stochastic model. The application of receding horizon control [11, 16] is investigated. Robust receding horizon control algorithms are well known for linear systems [5, 2]. However, the air-operation model discussed here is non-linear.

A variable substitutiolinearizes the nonlinear terms determining the dynamics of the system. Although control variable constraints on the system remain non-convex, the linearized dynamics allow consideration of uncertainties within the model. By exploiting the structure of the system, the optimization problem is further simplified resulting in a problem that grows linearly with the horizon length. Robust solutions are calculated in both open-loop and state-feedback. The solution found in [20] is shown to be resilient to the uncertainties introduced.

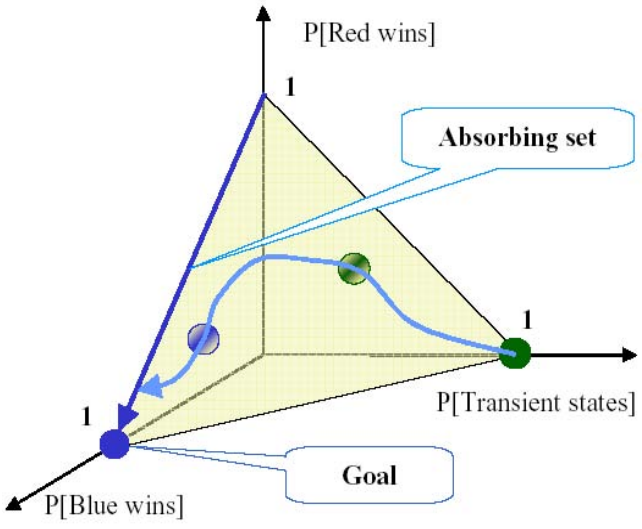

Figure 1 Concept of control to win on a probability simplex.

The paper is organized as follows. Section 1.2 details a strategic model in a form suitable for control purpose and examines some basic properties of the model. Section 1.3 formulates and solves a receding horizon control problem based on the strategic model. Simulations of the optimal policy are conducted with and without state variable feedback. Section 1.4 presents the results and compares the performance when considering model uncertainty. Conclusions are drawn in Section 1.5, and the possibility of further work is presented.

1.2 Modeling for Control

This section presents a strategic model derived from two extremal models [19] of differing aggressiveness of Blue. With appropriate assignment of parameters, the simple model is sufficiently general to represent most military air operations at the strategic level with an arbitrary degree of Blue's aggressiveness relative to Red's.

Unlike most existing efforts in hierarchical hybrid modeling [1], [19] focused on encapsulating the interactions between the strategic and the tactical operations, where the interactions are captured in the transition coverage parameters. This section will transform the transition parameters into control variables that enable dynamic strategic planning via state-feedback, and produce a strategic model suitable for control design.

1.2.1 Stochastic Model of Air Operation

The strategic model is in the form of a controlled non-homogeneous Markov chain. Specifying a Markov chain model requires the definition of a state-space X, a probability mass distribution $\pi(0)$ for the initial state, and a set of transition rates $\{\lambda_{x,x'}\}$ from x to x', where $x, x' \in \mathrm{X}$ [7]. As in [19], the state-space of the strategic model is constructed from the composition of binary states: Blue threatened, Blue defeated, Red threatened, and Red defeated. Fig. 2 shows the rate transition diagram of the model. With '1' denoting true and '0' denoting false, the state space contains two absorbing states {0001, 0100}, representing the defeat of a force, and four transient states {0000, 0010, 1000, 1010}. The state-space can also be represented in decimal form as {1, 4, 0, 2, 8, 10}, arranged from the absorbing group to the transient group in ascending order within each group according to the assigned decimal numbers.

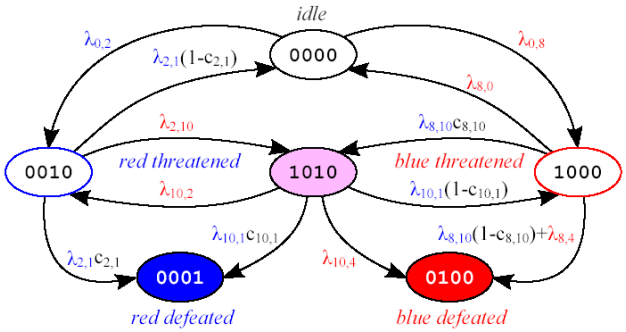

Figure 2 A low resolution strategic model.

It is assumed that the air operation always initializes to the idle state $x = 0$. Hence, the initial probability mass distribution is given by $\pi(0) = (0,0,1,0,0,0)$. Arrival at one of the absorbing states ends the air operation. The objective of the strategic plan is to maximize Blue's probability of winning. Therefore, a victory corresponds to the arrival at the absorbing set $x = 1$, or the defeat of Red. Likewise, arrival at the absorbing set $x = 4$ corresponds to Blue's defeat.

Transition rates $\{\lambda_{x,x'}\}$ are traditionally determined based on the first principle in terms of the remaining assets [8], or derived from Poisson clock structures that define the arrivals of triggering events [18]. The transition rates in Fig. 2 are inherited from [19], and are shown in Table 1 where competition between Red and Blue is fostered by setting the rates of occurrence of similar events near equal.

Table 1 Numerical values (in hours) for transition rates in Fig. 2.

$\lambda_{0,2}$	$\lambda_{2,10}$	$\lambda_{10,2}$	$\lambda_{2,1}$	$\lambda_{0,8}$	$\lambda_{8,0}$	$\lambda_{8,4}$	$\lambda_{8,10}$	$\lambda_{10,4}$	$\lambda_{10,1}$
.2	.2	.02	.3	.2	.02	.04	.4	.005	.05

In Fig. 2, $c_{x,x'}(t)$ denotes the transition coverage associated with a transition from x to x'. It depends on the conditional probability $p_{x'|x}(t)$ that the transition will take place given that a triggering event has occurred. With $\lambda_{x,x'}$ assumed to be time invariant, $c_{x,x'}(t)$ can be expressed as

$$c_{x,x'}(t) = \frac{1}{t}\int_0^t p_{x'|x}(\tau)d\tau, \tag{1.1}$$

using the Poisson decomposition property [9]. It can be seen that $0 \le c_{x,x'}(t) \le \max_t p_{x'|x}(t) \le 1$. In addition, if $p_{x'|x}(t)$ is non-decreasing in t, so is $c_{x,x'}(t)$. The corresponding transition rates vary according to $\lambda_{x,x'}c_{x,x'}(t)$. The resulting Markov process is homogeneous only when $p_{x'|x}(t)$ is independent of time, in which case $p_{x'|x} = c_{x,x'}$.

Let the elements of vector

$$\boldsymbol{\pi}(t) = \begin{bmatrix} \pi_1(t) & \pi_4(t) & \pi_0(t) & \pi_2(t) & \pi_8(t) & \pi_{10}(t) \end{bmatrix}$$

denote the probabilities of being in a corresponding state at time t. Assume for the moment that all $c_{x,x'}(t)$'s are independent of time. State transition matrix function $\mathbf{P}(t)$ can be determined through the forward Kolmogorov equation [9]

$$\dot{\mathbf{P}}(t) = \mathbf{P}(t)\mathbf{Q}, \qquad \mathbf{P}(0) = \mathbf{I}, \tag{1.2}$$

where the off diagonal elements of Q in (1.2) are given in Table 2, and the diagonal elements are determined by summing up the elements in each row to zero in the transition rate matrix. The state probability vector can be shown to satisfy

$$\dot{\boldsymbol{\pi}}(t) = \boldsymbol{\pi}(t)\mathbf{Q}. \tag{1.3}$$

Table 2 Non-zero off-diagonal entries of transition rate matrix Q.

$q_{0,2}$	$\lambda_{0,2}$
$q_{0,8}$	$\lambda_{0,8}$
$q_{2,1}$	$\lambda_{2,1}c_{2,1}$
$q_{2,0}$	$\lambda_{2,1}(1-c_{2,1})$
$q_{2,10}$	$\lambda_{2,10}$
$q_{8,4}$	$\lambda_{8,10}(1-c_{8,10})+\lambda_{8,4}$
$q_{8,0}$	$\lambda_{8,0}$
$q_{8,10}$	$\lambda_{8,10}c_{8,10}$
$q_{10,1}$	$\lambda_{10,1}c_{10,1}$
$q_{10,4}$	$\lambda_{10,4}$
$q_{10,2}$	$\lambda_{10,2}$
$q_{10,8}$	$\lambda_{10,1}(1-c_{10,1})$

Table 3 Steady-state effects of Blue's aggressiveness with different amounts of resources.

$\lambda_{0,2}$	$c_{8,10}$	$c_{10,1}$	$c_{2,1}$	**Blue Wins**	**Red Wins**
0.6	1.0	1.0	1.0	0.94	0.06
0.2	1.0	1.0	1.0	0.91	0.09
0.0	1.0	1.0	1.0	0.84	0.16
0.6	0.5	0.5	0.8	0.70	0.30
0.2	0.5	0.5	0.8	0.56	0.44
0.0	0.5	0.5	0.8	0.29	0.71

To gain some insight into how the strategic operation depends on the control variables, the results for selected constant values of $c_{8,10}, c_{10,1},$ and $c_{2,1}$ are shown in Table 3.

Table 3 shows the effect of Blue's aggressiveness, modeled by $\lambda_{0,2}$, on the outcome of the strategic operation. With fully adequate resources $c_{8,10}=c_{10,1}=c_{2,1}=1$, the winning probability increases by 12% when Blue is three times as fast in engaging itself at the onset $(\lambda_{0,2}=3\times 0.2)$. Blue's aggressiveness more than doubles its probability of winning with an increase of 141% when resources are somewhat inadequate $(c_{8,10}=c_{10,1}=0.5, c_{2,1}=0.8)$.

1.2.2 Bilinear and Input Constrained Design Model

It can be see from Fig. 2 that all nontrivial transitions $x\to x': 8\to 10, 10\to 1,$ and $2\to 1$ that can be influenced by Blue have control variables attached. When a planned action associated with a transition is somehow disabled, the value of the corresponding control strategic model is set to 0. Note that the strategic model in the form of a Markov chain describes the average stage. The description becomes more accurate for a particular realization if state information acquired in real-time is available, which allows reinitialization of the model periodically. The information on strategic state, however, is generally severely deficient, and the reduction of uncertainty comes at a cost of time required for data acquisition, processing, and decision making. An error in decision leads to an undesirable transition, indicated by a rate attached with a $\bar{c}_{x,x'}=1-c_{x,x'}$.

This paper assumes a nondecreasing temporal profile for conditional probability $p_{x'|x}(t)$. Therefore, from (1.1) control variable $c_{x,x'}(t)$ is also nondecreasing. This is intended to capture the process of information acquisition and the process of execution of the strategic plan at the tactical level. In addition, the total rate at which $c_{x,x'}(t)$ increases is also constrained due to limited resources that are allocated and the time required to estimate the strategic state. Under the fixed total rate, distribution of resources becomes a constrained control problem.

Equation (1.3), that governs the evolution of strategic state probability, is now rewritten as

$$\dot{\boldsymbol{\pi}}(t) = \mathbf{A}\boldsymbol{\pi}(t) + \mathbf{B}(\boldsymbol{\pi})\mathbf{u}(t), \quad \mathbf{A} = \mathbf{Q}'|_{c_{x,x'}=1} \tag{1.4}$$

where state $\boldsymbol{\pi}'(t)$, control

$$\mathbf{u}(t) = \begin{bmatrix} c_{10,1}(t) & c_{8,10}(t) & c_{2,1}(t) \end{bmatrix}', \tag{1.5}$$

$\mathbf{A} = \mathbf{Q}'|_{c_{x,x'}=1}$, and

$$\mathbf{B}(\boldsymbol{\pi}(t)) = \begin{bmatrix} \pi_{10}(t)\lambda_{10,10} & 0 & \pi_2(t)\lambda_{2,1} \\ 0 & -\pi_8(t)\lambda_{8,10} & 0 \\ 0 & 0 & -\pi_2(t)\lambda_{2,1} \\ 0 & 0 & 0 \\ -\pi_{10}(t)\lambda_{10,1} & 0 & 0 \\ 0 & \pi_8(t)\lambda_{8,10} & 0 \end{bmatrix}$$

The bilinear model expressed in (1.4)—(1.5), is inherently a stochastic system. Therefore, the state trajectory that evolves on the 5-dimensional probability simplex defined by

$$[\pi_1 + \pi_4 + \pi_0 + \pi_2 + \pi_8 + \pi_{10}](t) = 1, \quad \pi_i(t) \geq 0, \forall i$$

always converges to a point on the 1-dimensional segment defined by $\pi_1(\infty) + \pi_4(\infty) = 1$ and $\pi_0 = \pi_2 = \pi_8 = \pi_{10} = 0$. The challenge is clearly seen now as how to determine a control policy that maximizes π_1 or minimizes π_4.

1.2.3 Modeling Uncertainty

Previously assuming transition rates are based on known, exponentially distributed rates in [20] limits the analytical value of the results. Reduced modeling knowledge of the opposing forces results in uncertain rates with regard to Red. Hence, rates $\lambda_{0,8}, \lambda_{8,0}, \lambda_{2,10}, \lambda_{10,2}, \lambda_{8,4}$, and $\lambda_{10,4}$ carry potential uncertainties. Although practical situations may impose uncertainty on Blue's own abilities, $\lambda_{0,2}, \lambda_{2,1}, \lambda_{10,1}$, and $\lambda_{8,10}$ involve no uncertainty within this exercise.

1.2.3.1 Uncertainties as disturbances

The original proposal suggested that the uncertainties would be modeled as disturbances in the nominal plant. The resulting bilinear state space equation resembled

$$\dot{\boldsymbol{\pi}}(t) = \mathbf{A}\boldsymbol{\pi}(t) + \mathbf{B}(\boldsymbol{\pi})\mathbf{u}(t) + \mathbf{F}\mathbf{w}(t) \tag{1.6}$$

where $\mathbf{w}(t)$ is a random, bounded uncertainty and $\mathbf{F}$ is a matrix defining the effects of uncertain rates on the plant.

The nonlinear plant hindered min-max optimization of the uncertain system. Quantifying the effects of disturbances on a nonlinear plant also proved difficult. Ultimately without bounding the sum of the disturbances to equal zero, the state-space of the system will add up to a value not equal to one. This was not desirable after considering that the state-space represents a probability space.

1.2.3.2 Polytopic, bounded rates

All uncertain rates, $\delta_{x,y}$, from state x to y are assumed be constrained by a box. Upper and lower bounds limit the uncertainty within each state transition.

$$\lambda_{x,y}^{\min} \le \delta_{x,y} \le \lambda_{x,y}^{\max} \tag{1.7}$$

Modeling the rates in this manner results in polytopic uncertainties. Polytopes contain the uncertain set of possible states at any given time.

1.3 Control of Strategic Operation

Control design for a strategic model offers a way to generate a set of strategic state-dependent dynamic specifications to be imposed on the tactical operation, which is executed to maximize Blue's chance of winning. This section considers the formulation and solution of a control problem for the model described in (1.4)–(1.6). On-line implementation of the control policy and the performance of the controlled process are also discussed.

Control Problem Formulation: An optimal control problem is formulated to be solved at each step of the on-line receding horizon implementation. The principles of Markov decision processes and dynamic programming are applied to the Markov chain model of an air operation with continuous control inputs instead of decision variables. A variable substitution is performed in order to facilitate the solution of a min-max optimization. This effectively maximizes the objective function for the worst case perturbation.

1.3.1 Modeling for Dynamic Programming

To facilitate analytical results and optimal solutions, a dynamic program is formed similar to a Markov decision process [7]. As such, the process is uniformized [7] at rate γ. A cost or reward, $C(x,\mathbf{u}_k)$, is assigned to accumulate over time in each state $x \in \mathrm{X}$ given the current control input $\mathbf{u}_k$. Instead of binary decision variables required by a true Markov decision process, control variables $c_{x,y}$ determine the propagation of the chain. The cost-to-go in state $x, v_{x,k}$ is calculated at each step, k, of the dynamic program by [7]:

$$v_{x,k-1} = R(x,\mathbf{u}_k) + \sum_{y \in \mathrm{X}} p_{x,y}(\mathbf{u}) v_{y,k+1} \tag{1.8}$$

where $p_{x,y}(\mathbf{u})$ is the probability of a transition from x to y uniformized with rate γ.

Due to the absorbing nature of states {1,4}, their cost-to-go values are constants determined prior to optimization. Hence, for the purpose of optimization, the system is reduced from six equations to four equations shown relaxed to inequalities by (1.11)-(1.14). The reduction of equations also reduces computational complexity of the resulting optimization problem.

The dynamic programming formulation is later used for a min-max optimization step (1.9)-(1.19) of the receding horizon control algorithm. Either the cost is minimized or the rewards are maximized for the worst case disturbance. Adding state constraints to the optimization is not necessary because the dynamics of the process naturally constrain the state space to the probability plane. (1.16)-(1.19) are introduced to constrain the control input. It must be non-decreasing, (1.18), limited in its rate of increase by Δu, (1.16), no larger than one (1.17), and initially equal to its current value (1.19).

$$\max_{\mathbf{u}} \min_{\delta} \ \boldsymbol{\pi}_0^{'} \mathbf{v}_0 \tag{1.9}$$

Subject to: $v_{i,N} = P(\text{blue wins} | x_N = i)$ for $i \in \{0,2,8,10\}$. (1.10)

$$v_{0,k-1} \le \left[1 - \frac{\lambda_{0,2} + \delta_{0,8}}{\gamma}\right] v_{0,k} + \frac{\lambda_{0,2}}{\gamma} v_{2,k} + \frac{\delta_{0,8}}{\gamma} v_{8,k}, \tag{1.11}$$

$$v_{2,k-1} \le \left[1 - \frac{\lambda_{2,1} + \delta_{2,10}}{\gamma}\right] v_{2,k} + \frac{\delta_{2,10}}{\gamma} v_{10,k} + \frac{\lambda_{2,1} c_{2,1,k}}{\gamma} 1 + \frac{\lambda_{2,1}(1 - c_{2,1,k})}{\gamma} v_{0,k}, \tag{1.12}$$

$$v_{8,k-1} \le \left[1 - \frac{\lambda_{8,10} + \delta_{8,0} + \delta_{8,4}}{\gamma}\right] v_{8,k} + \frac{\delta_{8,0}}{\gamma} v_{0,k} + \frac{\lambda_{8,10} c_{8,10,k}}{\gamma} v_{4,k}, \tag{1.13}$$

$$v_{10,k-1} \le \left[1 - \frac{\lambda_{10,1} + \delta_{10,4} + \delta_{10,2}}{\gamma}\right] v_{10,k} + \frac{\delta_{10,2}}{\gamma} v_{2,k} + \frac{\lambda_{10,1} c_{10,1,k}}{\gamma} 1 + \frac{\lambda_{10,1}(1 - c_{10,1,k})}{\gamma} v_{8,k}, \tag{1.14}$$

where $\lambda_{x,y}^{\min} \le \delta_{x,y} \le \lambda_{x,y}^{\max}$ (1.15)

$$\sum_{n=1}^{3} u_{n,k} - \sum_{n=1}^{3} u_{n,k-1} \le \Delta u, \tag{1.16}$$

$$0 \le u_{x,y,k+1} \le 1, \tag{1.17}$$

$$u_{n,k} \ge u_{n,k-1}, \tag{1.18}$$

$$u_{n,0} = u_{n,i} \ \text{ for } \ n \in \{1,2,3\}. \tag{1.19}$$

If current state $j \in \{0,2,8,10\}$ is observed, initial condition $\mathbf{x}_k$ in (1.10) is assigned a pmf $\delta_j (\pi_j = 1, \text{ and } \pi_l = 0, l \ne j)$, and the next iteration for control update begins by solving the constrained optimization problem (1.9)-(1.19).

This corresponds to the closed-loop operation to be further discussed in the next subsection. Otherwise, the process iterates in open-loop based on the strategic model, and uses the resulting probability calculated from (1.6) with $i = 0$ as the initial condition of the next optimization for control update. Note that the controlled Markov chain based on the strategic model does not involve feedback of the current state of any realization of the corresponding stochastic process.

1.3.2 Cost Structure

1.3.3 Solution of Min-Max Optimization

Unless the structure of the problem is exploited, non-linear min-max problems are extremely difficult to solve. Generally, the objective function is maximized for each possible set of disturbances. The solution is the set of disturbance values and maximization variables that result in the smallest value of the individual maximization problems. Modeling the uncertainties as polytopes substantially decreases the problem's complexity. When uncertainties lie within a polytope, the worst-case uncertainty is always located on one of the vertices [5]. Hence, it is only necessary to maximize the objective function for each vertex of the uncertainty set. The number of vertices grows exponentially with the horizon length.

The problem further simplifies by applying the following theorem from [3]:

Theorem 1 (Bertsekas [3]) *Let* $\square$ *be a closed convex set and let* $f:\square \to \square$ *be a convex function. Then if* f *attains a maximum over* $\square$ *, it attains a maximum at some extreme point of* $\square$.

Similar relationships simplify robust receding horizon control of linear systems [5]. For the nonlinear set of relationships in (1.11), the theorem does not hold. The structure of the problem allows for feedback linearization [10]. The transition coverage variable are replaced by substituting $u_{h,k} = s_{h,k} / v_{j,k}$ and $1-u_{h,k} = s_{h+3,k} / v_{l,k}$ where $h = 1,2,3$ and j, l are selected to cancel the cost-to-go term in term corresponding to control variable $u_{h,k}$ or $1-u_{h,k}$, respectively. An addition set of restraints requires that $s_{h,k} / v_{j,k} = 1 - s_{h+3,k} / v_{l,k}$. The critical relationship between uncertainty sets, (1.11), is now convex and, more specifically, affine.

The structure of the problem is further exploited to reduce the size of the optimization problem. The optimality equations of a Markov decision problem are typically constrained by equalities. Due to the desire to minimize the cost (and a lack of any competing force) at every stage of the problem, the constraints in (1.11) are relaxed to inequalities forcing a lower bound on the minimization. The worst-case scenario is enforced by providing an inequality constraint for each vertex of the uncertainty set. Bertsekas' theorem provides that only this worst-case need be found along each point of the horizon. The number of constraints in the problem now grows linearly with the horizon.

1.3.4 Closed-Loop Control with SimEvents Model in the Loop

This subsection discusses the on-line computation of control policy based on the observed strategic state. State-feedback requires implementation of the discrete state stochastic process as a superposition of Poisson arrival processes. Simulation of the process is performed under the Simulink environment [15] using the discrete event simulation package SimEvents [14].

Let $T_{l,n}$ denote the state holding time at strategic state $l \in \{0,2,8,10\}$ before transitioning to n, and t denote the time state $l \in \mathrm{X}$ is entered. It can be shown that $T_{l,n}$ obeys the following distribution [9]:

$$F_{T_{l,n}}(\tau \mid t) = 1 - e^{-[m_{l,n}(t+\tau) - m_{l,n}(t)]}, \quad \tau > 0, \tag{1.20}$$

where $m_{l,n}(t)$ is specific to event $e_{l,n}$. For example, corresponding to transition rate $\lambda_{l,n} c_{l,n}(t)$

$$m_{l,n}(t) = \int_0^t \lambda_{l,n} c_{l,n}(\sigma) d\sigma. \tag{1.21}$$

Upon entering l, occurrence times of all activated events can be calculated using the inverse transform method based on (1.20). By setting the right hand side of (1.20) to a random number, r sampled from a uniform distribution defined on $[0,1]$, random occurrence time $T_{l,n} = \tau_{l,n}$ can be solved.

Let $\{\boldsymbol{\mu}(\boldsymbol{\pi}_k)\}$ denote the control policy derived from the receding horizon control problem (1.9)-(1.19) for each initial condition assigned and $\mu_{l,q}(\boldsymbol{\pi}_k)$ denote the component of $\boldsymbol{\mu}(\boldsymbol{\pi}_k)$ (which can be $c_{l,q}(t_k)$, $1-c_{l,q}(t_k)$, or 1) associated with transition from current state $l \in \{0,2,8,10\}$ to next state $q \in \mathrm{X}$. In an open-loop setting, initial condition $\boldsymbol{\pi}_k$ in (1.10) is computed using (1.20) driven by $\boldsymbol{\mu}(\boldsymbol{\pi}_{k-1})$. In a closed-loop setting, initial condition $\boldsymbol{\pi}_k$ is an assigned probability mass distribution function δ_l ($\pi_l = 1$, and $\pi_q = 0, \forall q \neq l$), where state $l \in \mathrm{X}$ is observed from the stochastic process driven by $\boldsymbol{\mu}(\boldsymbol{\pi}_{k-1})$. The process terminates if $l = 1$ or $l = 4$.

The need for the on-line update of the control variable $c_{l,q}(t)$ complicates the computation of the next state transition time because $m_{l,q}(t)$ is known only up to the time the control variable that depends on the random strategic state is updated. If the strategic state information is acquired as frequently as control update, the solution for $\tau_{l,q}$ can be searched at each iteration as follows. Setting the right hand side of (1.20) equal to $r \in U[0,1]$ results in

$$\tau_{l,q} = g^i_{l,q}(t) \big/ \mu(\boldsymbol{\pi}_{k+i-1}) - t, \quad i = 1,2,\cdots, \quad t \le t_k \tag{1.22}$$

where

$$g^i_{l,q}(t) = -\frac{\log(1-r)}{\lambda_{l,q}} + \frac{k+i-1}{\gamma}\mu_{l,q}(\boldsymbol{\pi}_{k+i-1}) - \left[\frac{k}{\gamma} - t\right]\mu_{l,q}(\boldsymbol{\pi}_{k-1}) - \frac{1}{\gamma}\sum_{p=0}^{i-1}\mu_{l,q}(\boldsymbol{\pi}_{k+p}). \tag{1.23}$$

Solution $\tau \ge 0$ exists as soon as the right hand side of (1.23) becomes nonnegative. Based on this observation an algorithm is established that calculates the state holding time at l and the next state $n \in \mathrm{X}$. A sample execution of Algorithm 1 is illustrated in Fig. 3.

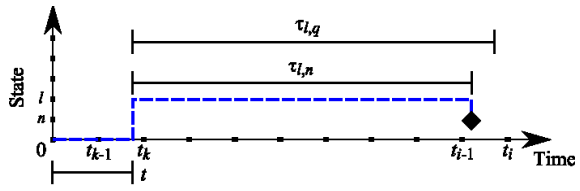

Figure 3 An execution of Algorithm 1. Both $t + \tau_{l,q}$ and $t + \tau_{l,n}$ result in a state transition before the next control update. However, the event associated with $t + \tau_{l,n}$ occurs first.

Algorithm 1:

1) State l is entered at $t_{k-1} < t \le t_k$; $i = 0$;
2) $i = i + 1$;
3) Calculate $\mu_{l,q}(\boldsymbol{\pi}_{k+i-1})$ by solving (1.9)-(1.19);
4) If $\mu_{l,q}(\boldsymbol{\pi}_{k+i-1})(k+i)/\gamma \le g^i_{l,q}(t)$ for all q, then iterate on the next control update: i. Goto 2;
5) Otherwise iterate on the next feasible transition:
   i. $t = t + \min_q \tau_{l,q}$;
   ii. $n = \arg\min_q \tau_{l,q}$;
   iii. Goto 1;

Example samples paths of the algorithm under nominal parameters are available in [20,17].

1.3.5 Results

1.3.5.1 Open-Loop Policy

Open-loop simulations are conducted using the nominal values of Blue's rates, $\lambda_{0,2}, \lambda_{2,1}, \lambda_{10,1}$, and $\lambda_{8,10}$, in Table 1 and uncertain Red rates, $\lambda_{0,2}, \lambda_{2,1}, \lambda_{10,1}$, and $\lambda_{8,10}$, within the range $0.5\lambda_{x,y} \le \delta_{x,y} \le 3\lambda_{x,y}$. The uniform rate is set to $\gamma = 1$ hour which corresponds to a sampling rate of one hour. $f_{\min con}$, provided in the Optimization Toolbox of MATLAB [13], solves the nonlinear optimization problem at each step of the horizon.

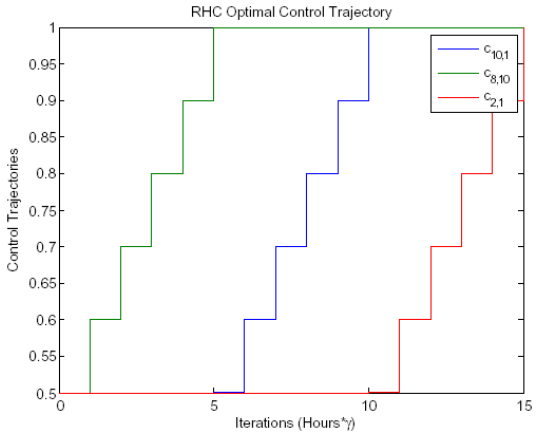

Figure 4 The optimal, open-loop control trajectory solved under nominal parameters of the air operation.

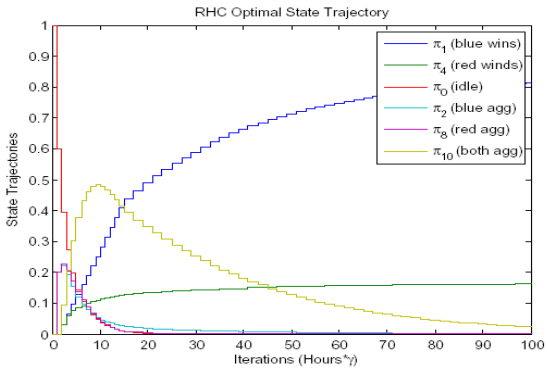

Figure 5 The optimal, open-loop probability trajectory solved under nominal parameters of the air operation.

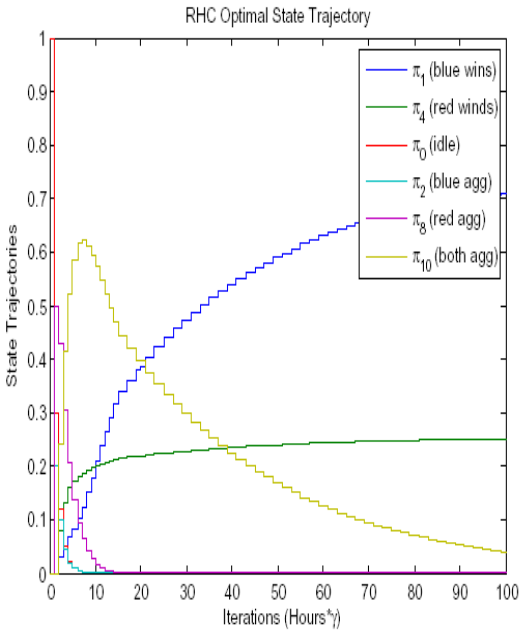

Figure 6 The optimal, open-loop probability trajectory solved with uncertain transition rates in the air operation.

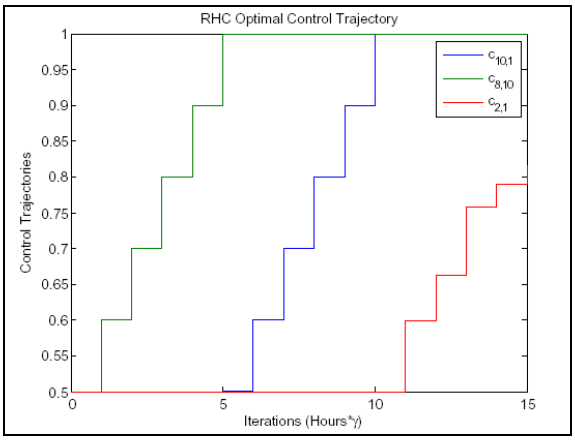

Figure 7 The optimal, open-loop control trajectory solved with uncertain transition rates in the air operation.

Figures 4 and 5 plot the nominal, optimal control and probability trajectories without consideration for uncertainties. With uncertainties in the optimization, the results are plotted in Figures 6 and 7. The probability trajectories in Figure 7 are calculated for the worst-case uncertainties. Even given the possibility of uncertainties with the model, the control trajectory demonstrates its robustness by remaining the same in Figures 5 and 7. The plots indicate that Blue wins 83.72% of the time under nominal parameters. Under the worst case uncertainty, Blue is only able to achieve victory 72.98% of the time.

1.3.5.2 Closed-Loop Policy

Table 4 Probabilities of Victory Under Nominal Parameters and Closed-loop Policy.

Policy	Win Percentage
Nominal Policy	86.10%
Robust Policy	84.07%

Table 4 contains the results of the closed-loop simulations. Both the nominal and robust policies are solved and executed against the air-operation model. The results are averaged over 1000 event simulation based on the Law of Large Numbers [6]. In this case, accounting for uncertainties slightly reduces the performance of the air operation. This reduction is small considering that advantages of robust planning.

2. Robust Tasking of Wireless Airborne Networks

The objective of the proposed research is to develop robust tasking policies for a network of clustered airborne vehicles deployed to carry out an ISR (intelligence, surveillance, and renaissance) mission in a hostile environment. These vehicles function as a part of a C3 (command, control, and communications) assembly. We envision an architecture where each cluster has multiple vehicles in formation. They cooperatively perform their tasks, among them cooperative communications, in the face of loss of vehicles, fading of channels, and intercept of information by adversaries.

Task allocation of airborne vehicles has gained much attention recently [21]. Examples of tasks include target conformation, target removal (by strike craft), and confirmation of the removal, as considered by Bailey, Tavana, and Busch [22]. This research proposes to resolve two important remaining issues that pertain to task allocation. The first issue is associated with communications among the clusters. This issue has been, to varying degrees, trivialized in the task-allocation research. The second issue is the consideration of uncertainties in the evolution of an air operation, which greatly impact the outcome of task allocation. A major source of such uncertainties is attributable to the lack of reliability and security in communications, especially in the presence of adversaries.

The focus of our effort during the first summer for this 3-year research project is on establishing a framework for our study, suitable for the design of tasking policies for clustered cooperative activities in a dynamic uncertain environment. Since secure and reliable communication is essential in this setting, tasking is to be confined to that relevant to cooperative communications.

In order to set up the multi-hop clustered cooperative transmission framework, in Section 2.1 we first set up models for single-link transmissions, where we consider especially two clustered single-link transmission schemes: conventional beamforming and a new secure transmission scheme. Then in Section 2.2 we set up a model for multi-hop wireless transmission, and by integrating with the clustered cooperative single-link transmission schemes, we outline a multiple objective optimization framework to determine networking parameters. These models and optimization frameworks are then studied numerically by simulations in Section 2.3. In Section 2.4 we include network reliability as a new objective when formulating the multiple objective optimization frameworks. Finally, a conclusion is given in Section 2.5.

2.1 Single-link transmission models

In this section, we set up and compare single link transmission models. Specifically, we first introduce a new secure transmission scheme [23], and then describe the conventional beamforming [24]. Both of them are clustered cooperative transmissions using distributed communication nodes with single antenna. The models are described based on the comparison with the conventional single-antenna transmissions [25].

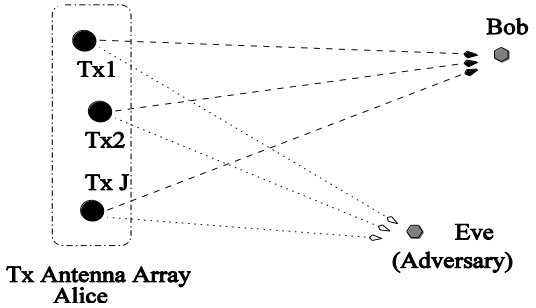

Figure 8 With a new clustered cooperative secure transmission scheme, Alice can transmit signals to Bob securely against eavesdropper Eve.

2.1.1 A clustered secure transmission scheme

Consider a cluster of J transmitters, each transmitter having a single transmit antenna. This cluster of transmitters transmits a data packet to another cluster of J receivers, each with a single receiving antenna. We assume that the transmitters or receivers may not share their received signals within cluster for joint receiving processing (because otherwise the bandwidth required for sharing raw sample data may be too high). But they can exchange data packet or control information so each receiving antenna has to process its received signal alone.

The received signal in our secure transmission scheme can be written as

$$y(n) = \mathbf{h}^H \mathbf{w}(n) b(n) + v(n) \tag{2.1}$$

where $y(n), b(n), v(n)$ are scalar received sample, transmitted symbol, and noise sample, respectively. $\mathbf{h}, \mathbf{w}(n)$ are $J \times 1$ vectors of channel and secure transmission encoding vectors, respectively, i.e.,

$$\mathbf{h} = \begin{bmatrix} h_1 \\ \vdots \\ h_J \end{bmatrix}, \quad \mathbf{w}(n) = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix}. \tag{2.2}$$

The actually transmitted signal can be written as

$$\mathbf{x}(n) = \mathbf{w}(n) b(n). \tag{2.3}$$

So the transmission power depends on the correlation matrix of the vector $\mathbf{x}(n)$.

The encoding vector is calculated based on the channel information. Note that the receiver can get channel information from channel feedback or channel reciprocity. One of the detailed forms for calculating the encoding vector is as follows

$$\mathbf{w}(n) = \mathbf{P}_i(n) \begin{bmatrix} a_i - \mathbf{f}_i^H \mathbf{z}_i(n) \\ \mathbf{z}_i(n) \end{bmatrix} \tag{2.4}$$

where the $J \times J$ matrix $\mathbf{P}_i(n)$ is a permutation matrix whose function is to insert the first row of its following vector into the i^{th} row, and the rest of the variables are

$$\begin{aligned} a_i &= \frac{1}{h_i^*} \|\mathbf{h}\|, \\ \mathbf{f}_i &= \frac{1}{h_i} \begin{bmatrix} h_1 & \cdots & h_{i-1} & h_{i+1} & \cdots & h_J \end{bmatrix}^T \\ \mathbf{z}_i(n) &= \begin{bmatrix} w_1(n) & \cdots & w_{i-1}(n) & w_{i+1}(n) & \cdots & w_J(n) \end{bmatrix}^T \end{aligned} \tag{2.5}$$

With such an encoding method, the received signal at the targeting user (who has channel $\mathbf{h}$) becomes

$$y(n) = ab(n) + v(n) \tag{2.6}$$

So the receiver can detect the symbol simply as

$$\hat{b}(n) = a^{-1} y(n). \tag{2.7}$$

The receiving performance in terms of SNR or BER is the same as a conventional beamforming with J receiving (or transmitting) antennas. We can use as comparison basis the single-antenna to single-antenna transmission's SNR γ and BER P_e. The BER and SNR relation ship of this single antenna case can be the following approximations:

$$P_e \sim Q(\sqrt{\lambda}) \text{ (in AWGN channels) or } P_e \sim \gamma^{-1} \text{ (in fading channels)}$$

In our secure transmission, according to the concept of array gain, the average SNR of the targeting receiver will be

$$\gamma_{\text{secure}} = J\gamma \tag{2.8}$$

when we use BER as evaluation metric, the BER in our case becomes

$$P_{e,\text{secure}} \sim Q(\sqrt{J\gamma}). \tag{2.9}$$

However, we may also use the following as approximation:

$$P_{e,\text{secure}} \sim \gamma^{-J} \tag{2.10}$$

from which we can clearly see the advantage of diversity J (which equals to the number of transmit/receive antennas). Therefore, the secure transmission can enhance the secure link's SNR or reduce the secure link's BER.

The cost paid is a higher transmission power. Let the conventional single-antenna to single-antenna's transmission power be P_t. Then the secure transmission method's transmission power can be approximately written as

$$P_{t,\text{secure}} = (2J-1)P_t. \tag{2.11}$$

Note that this transmission power can be in general from 0 to infinity. Its size depends on the parameters we used in calculating the encoding vectors $\mathbf{w}(n)$. But the above equation is a typical value for some typical choice of the parameters.

Obviously, using clustered secure transmission means longer transmission distance because increased SNR (or reduced BER), which also means that the number of hops in the network will be smaller. This will save some transmission power. But we still expect a relatively higher total power used when compared with single-antenna transmissions.

Another point is that each secure transmission can be made only from a cluster of J transmitters to ONE of the receivers in the receiver cluster. This is because we have assumed that the receivers do not share raw received signals for joint processing. Therefore, the same data packet has to be transmitted J times in order for all the receivers in the next cluster to have the same data. This will boost the total transmission power of one link from $P_{t,\text{secure}}$ to

$$P_{t,\text{each secure link}} = J(2J-1)P_t. \tag{2.12}$$

Note that such repeated transmission also means a $J-$fold reduced throughput (or data rate, or bandwidth efficiency) for the secure transmission. If the data rate of the single-antenna to single-antenna transmission is R, then the secure transmission would have data rate

$$R_{\text{secure}} = \frac{R}{J}. \tag{2.13}$$

The above development is based on the assumption that each secure transmission has the same data rate as single-antenna transmission, but has a longer transmission distance. So the higher transmission power is paid on longer distance and security. An alternative way to describing such relationship is to assume that the transmission distance of the secure transmission keeps same as single-antenna transmissions, so it can use a lower transmission power, or use a higher transmission data rate.

For all other users, the received signal can be written as

$$y_e(n) = \mathbf{h}_e^T \mathbf{w}(n) b(n) + v_e(n). \tag{2.14}$$

The vector $\mathbf{h}_e$ is the channel vector of the eavesdropper, and it is statistically independent from the encoding vector $\mathbf{w}(n)$. As a result, the random encoding vector $\mathbf{w}(n)$ will randomize the eavesdropper's signal, which makes the eavesdropper impossible to detect the symbols $b(n)$, hence the guaranteeing of transmission security.

The SNR of the eavesdropper is not meaningful. In fact, following the concept of beamforming (attenuating the eavesdroppers' received signal strength), then the SNR of $y_e(n)$ is actually increased by $2J-1$. However, because the eavesdropper can not resolve the random vector $\mathbf{w}(n)$, such SNR is useless. However, this observation indicates another problem: the secure transmission may interference other hop transmissions because its interference is stronger in longer distances. When we take multi-hop multi-packet simultaneous transmission into consideration, we may need to address this issue. However, this can be skipped if we just consider one packet data forward along one multi-hop path.

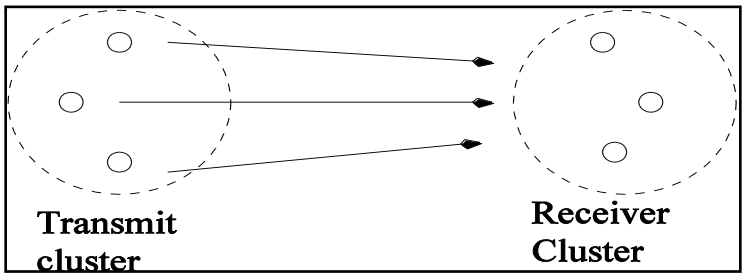

Figure 9 Illustration of beamforming transmission scheme where a clustered distributed transmission node forms a virtual transmit antenna array.

2.1.2. Clustered beamforming transmission scheme

Besides using the advanced secure transmission scheme, the clustered transmitters may also use conventional beamforming. In this section, we consider a typical beamforming scheme: transmit beamforming, i.e., the clustered transmitters utilize the channel knowledge to strengthen the signals targeting a desired user, while simultaneously attenuating signals to all the other uses. Transmit beamforming can usually achieve optimal beamforming results, albeit the requirement of channel knowledge means certain channel feedback has to be implemented which causes extra complexity.

Consider a transmit cluster with J transmitters, which transmit the same data packet (possibly with certain different encoding) to another cluster of J receivers. While the J transmitters can do some joint encoding because they have the same data packet information, we assume each of the J transmitters can only conduct receiving and decoding independently. Joint decoding requires the receivers to cross talk for information exchange, which consumes extra bandwidth and power resource. Therefore, we consider multi-input single-output (MISO) transmission model, instead of the more general multi-input multi-output (MIMO) model.

Each of the J transmitters knows the symbol sequence $b(n)$ to be transmitted. Each of them can do some appropriate encoding before transmission. In a conventional transmit beamforming, the transmitters utilize the knowledge of the channels, which may be obtained via a channel feedback procedure, i.e., the receiver estimates the channel and sends back to the transmitter. Let the baseband discrete channel from the transmitter i to the receiver be h_i, where $i = 1, \cdots, J$. Then the transmitter i just transmits the signal

$$x_i(n) = h_i^* b(n). \tag{2.15}$$

The receiver then receives signal

$$y(n) = \sum_{i=1}^{j} h_i x_i(n) + v(n). \tag{2.16}$$

Define the channel vector and signal vector as

$$\mathbf{h} = \begin{bmatrix} h_1 \\ \vdots \\ h_J \end{bmatrix}, \qquad \mathbf{x}(n) = \begin{bmatrix} x_1(n) \\ \vdots \\ x_J(n) \end{bmatrix}, \tag{2.17}$$

respectively. Then the signal model can be deducted as

$$y(n) = \mathbf{h}^T \mathbf{x}(n) + v(n) = \|\mathbf{h}\|^2 b(n) + v(n). \tag{2.18}$$

In order to detect the symbol $b(n)$ from the received signal $y(n)$, the receiver just needs to estimate the channels h_i, calculate $\|\mathbf{h}\|^2$, and evaluate $\|\mathbf{h}\|^{-2} y(n)$ as the estimation.

In order to evaluate the performance of the beamforming scheme, without loss of generality, let us assume the channels h_i are independent complex Gaussian random variables with zero mean and unit variance. This is reasonable for the distributed transmitters in a cluster because their positions and distances are different and random which causes the phases of their signals to be independently random when arriving at the receiver. This is one of the major differences of the MISO beamforming model when compared to the more traditional phased-array beamforming model in which the phase differences among the array elements can usually be assumed as deterministic or identical.

As a comparison basis, we first list the transmission parameters for the case of single transmitter to single receiver transmission. In this case, the transmission power can be denoted as $P_t = \sigma_b^2$, and the SNR is $\gamma = \sigma_b^2 / \sigma_v^2$, where σ_b^2 and σ_v^2 are the variances of the random symbol sequence $b(n)$ and the noise $v(n)$, respectively. The bit-error-rate (BER) can be described approximately as $P_e \approx \gamma^{-1}$ or $P_e = Q\left(\sqrt{\gamma}\right)$. We also assume the data rate in this case to be R.

Now for the transmit beamforming case, the overall transmit power is

$$P_{t,\text{beamform}} = E\left[\left\|\mathbf{x}(n)\right\|^2\right] = JP_t, \tag{2.19}$$

which means the transmit beamforming uses J times more transmission power. In other words, each of the J transmitters simply keep the transmission power P_t. In this case, the SNR becomes

$$\gamma_{\text{beamform}} = \frac{E\left[\left\|\|\mathbf{h}\|^2 b(n)\right\|^2\right]}{E\left[\left\|v(n)\right\|^2\right]} = J^2\gamma. \tag{2.20}$$

In fact, we usually prefer to use another equivalent description, i.e., we can also say that the transmit beamforming scheme can use just an overall transmit power P_t (the same as the single-transmitter case)

$$P_{t,\text{beamform}} = P_t \tag{2.21}$$

to realize a J fold increase of SNR to $J\gamma$

$$\gamma_{\text{beamform}} = J\gamma. \tag{2.22}$$

Then BER can be then be calculated as

$$P_{e,\text{beamform}} \approx \gamma^{-J} \quad \text{or} \quad P_e = Q\left(\sqrt{J\gamma}\right). \tag{2.23}$$

The data rate is still R in the transmit beamforming.

Now consider the eavesdropper which similarly uses just one receive antenna. The received signal can be written as

$$y_e(n) = \mathbf{g}^T\mathbf{x}(n) + v_e(n) \tag{2.24}$$

where $\mathbf{g}^T = \begin{bmatrix} g_1 & \cdots & g_J \end{bmatrix}$ are the channel coefficients from the J transmitters to the eavesdropper. The channel coefficients g_i can also be modeled as independent Gaussian random variable with zero mean and unit variance, and are independent from the desired user's channels h_i. The signal $y_e(n)$ can be rewritten as

$$y_e(n) = \mathbf{g}^T\mathbf{h}^* b(n) + v_e(n) = \left(\sum_{i=1}^{J} g_i h_i^*\right) b(n) + v_e(n). \tag{2.25}$$

The SNR of the eavesdropper can be evaluated as

$$\gamma_e = E\left[\left|\sum_{i=1}^{J} g_i h_i^*\right|^2\right]\gamma = J\gamma, \tag{2.26}$$

which means that when the transmitters spend power JP_t, the eavesdropper can achieve an SNR $J\gamma$ while the desired user has SNR $J^2\gamma$.

In other words, if the transmitters just use an overall transmission power P_t, then the eavesdropper can only have an SNR γ, while the desired user's SNR is $J\gamma$. The desired user always has the diversity gain J over the eavesdropper. This fact can be exploited by the transmit beamforming to enhance transmission security. If the transmission security is the objective, then the beamforming scheme allows use-to-use a lower transmission power to reduce the eavesdroppers' SNR while keeping the desired user's SNR unchanged.

The eavesdropper's BER can be evaluated similarly as last section by using the SNR results.

Note that this result is more desirable than the beam-width concept of the traditional phase-array beamformer. However, this result is based on the assumption that the channel coefficients are completely independent. As long as the distance between two antennas is larger than a half of the carrier wavelength, this independence assumption is valid.

2.1.3 Miscellaneous issues regarding security and reliability

2.1.3.1 Complexity of exhaustive-search attack to the secure transmission scheme

For our secure transmission scheme, it is proved that any adversary can not do a meaningful attack based on channel estimation or symbol estimation. Therefore, the only way left for the adversary is to do an exhaustive search of the targeting user's channel. If the adversary can accidentally find the targeting user's correct channel coefficients, and if the adversary can successfully estimate and remove its own channels, then the adversary can exploit the channel knowledge to recover the transmitted signals. Obviously, the practicability of this attacked relies on the complexity of the exhaustive search of the target user's channels.

The target user's channel is unknown to the adversary, or can be assumed to be random to the adversary. The only way left for the adversary is then an exhaustive try of all possible channel coefficients. The target user's channel has J complex coefficients, which leads to the guess of $2J$ real numbers. In addition, in order to obtain a meaningfully low bit-error-rate (BER) after this attack, the accuracy of the guessed channel coefficients must also be high enough. For example, in order to guarantee a BER of 10^{-3}, the accurate must be equivalent to a quantization level of 32. In other words, each real value of in the channel coefficients must be quantized by 5 bits. In this example, we find that the complexity of the exhaustive search is

$$C = 2^{10J} \tag{2.27}$$

which means the search space is on the order of 2^{10J}. The larger the number of transmit antennas J, the higher the complexity of the exhaustive search attack. We can put this constraint into the optimization of the clustering problem.

2.1.3.2 Effect of lost nodes in a transmission cluster

The conventional beamforming is fairly robust to loss of clustering nodes. If one or more transmitting nodes in a cluster is lost, then we will just have a graceful degradation of performance. Specifically, if k of the J nodes are missing, then the transmission is reduced to $(J-k)$ transmitter beamforming instead of the original J transmitter beamforming.

However, to our secure transmission scheme, the loss of node effect is more severe than the conventional beamforming. Recall the encoding vector of the secure transmission scheme (1.4). The targeting user requires the complete coherent multiplication of the channel coefficients and also the complete cancellation of the random coefficients $\mathbf{z}_i(n)$. This can be inferred from the multiplication of the targeting receiver's channel $\mathbf{h}$ and the encoding factor $\mathbf{w}(n)$, which is

$$\mathbf{h}^H \mathbf{w}(n) = h_i^* a_i - \sum_{j=1, j\neq i}^{J} \hat{h}_j^* w_j(n) + \sum_{j=1, j\neq i}^{J} h_j^* w_j(n) \tag{2.28}$$

where we use $\hat{h}_j$ to denote the channel coefficients used in calculating $\mathbf{w}(n)$, and $w_j(n)$ are the entries of random vector $\mathbf{z}_i(n)$. If there are some nodes lost during transmission, this is equivalent to some h_j^* becomes zero.

If it is the i^{th} node, the most important node, becoming lost (or the i^{th} rows becomes zero), then the targeting receiver can not decode the signal successfully because the transmitted signal becomes zero. Fortunately, because the row selection in $\mathbf{w}(n)$, specifically the permutation matrix $\mathbf{P}_i(n)$ changes symbol by symbol, the loss of this important node in the cluster will cause an increase of BER to $1/J$.

On the other hand, if it is any node other than the i^{th} node that becomes lost, then this is equivalent to that some terms of $w_j(n)$ can not be successfully canceled. Such remaining random factors will contribute interference to the detector. The size of the this interference can be roughly treated as having a signal-to-interference ratio

$$SIR = \frac{J-1}{1}. \tag{2.29}$$

In general, if we have k such nodes lost, then we would see the SIR reduced to

$$SIR = \frac{J-k}{k}. \tag{2.30}$$

2.1.3.3 A possible reformulation of secure transmission scheme for robustness to node failure

From the analysis in Section 2.1.3.2, we have seen that the lost of the leading node (i.e., the i^{th} node) may have a detrimental effect to the targeting receiver. The BER will be as low as $1/J$ in this case. In order to mitigate this problem, we may need to put some redundancy into this case. The basic idea is that instead of choosing just one leading node, we may reformulate the problem into using k leading nodes. This is equivalent to say that from within the J transmitting nodes, we use $J-k$ nodes to transmit interference, while using the rest k nodes to transmit the information signal.

More specifically, we can select k channel coefficients with indices $i_1,\cdots,i_k$, and calculate the encoding vector as

$$\mathbf{w}(n)=\mathbf{P}_{i_1,\cdots,i_k}(n)\begin{bmatrix}\frac{1}{k}\left(a_{i_1}-\mathbf{f}_{i_1}^H\mathbf{z}_{i_1,\cdots,i_k}(n)\right)\\ \vdots\\ \frac{1}{k}\left(a_{i_k}-\mathbf{f}_{i_1}^H\mathbf{z}_{i_1,\cdots,i_k}(n)\right)\\ \mathbf{z}_{i_1,\cdots,i_k}(n)\end{bmatrix} \tag{2.31}$$

where the $J\times J$ permutation matrix $\mathbf{P}_{i_1,\cdots,i_k}(n)$ is to insert the first k rows of its following vector into the corresponding $i_1,\cdots,i_k$ rows, and the rest of the variables are

$$\begin{aligned}
&a_{i_\ell}=\frac{1}{h_{i_\ell}^*}\|\mathbf{h}\|, \qquad \ell=1,\cdots,k\\
&\mathbf{f}_{i_\ell}=\frac{1}{h_{i_\ell}^*}\begin{bmatrix}h_1 & \cdots & h_j & \cdots & h_J\end{bmatrix},\ \ell=1,\cdots,k; \qquad j\notin\{i_1,\cdots,i_k\}.\\
&\mathbf{z}_{i_1,\cdots,i_k}(n)=\begin{bmatrix}w_1(n) & \cdots & w_j(n) & \cdots & w_J(n)\end{bmatrix},\ j\notin\{i_1,\cdots,i_k\}
\end{aligned} \tag{2.32}$$

With this reformulation, if there is a failing node in the k leading nodes, then we lose $1/k$ useful information energy, while we have some interference that can not be canceled. Since usually the uncancelled interference may dominate the noise, we can evaluate the performance by the increase in SIR.

In the sequel, we derive an approximate way to evaluate the SIR in this case. Assume that each transmitter transmit approximately similar power. Then the lose of m of the k leading nodes can be approximately looked as we have reduced the useful information power to $k-m$ while we have increased the interference power to m. Therefore, the new SIR in this case becomes

$$SIR=\frac{k-m}{m}. \tag{2.33}$$

2.2 Multi-hop transmission models

2.2.1 Transmission and receiving powers and security measure

In Section 2.1, we focused on setting up models and performance metrics for single-hop transmissions, without even considering the transmission distance. In order to extend the consideration into multi-hop setting and to compare the effects of hop numbers, we have to consider the transmission power and transmission distances.

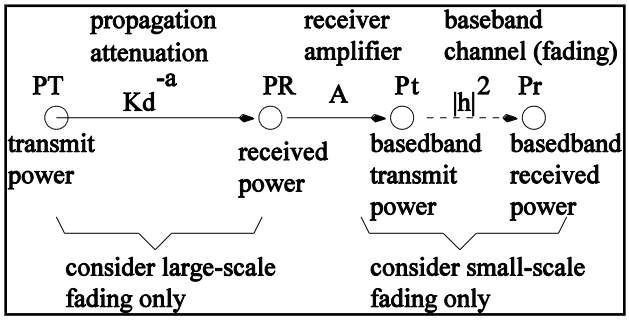

Figure 10 Illustration of real transmission/receiving power and baseband transmission/receiving power model.

For this purpose, we need first to clarify the relationship between the transmission powers defined in Section 2.1 (P_t, $P_{t,\text{secure}}$, and $P_{t,\text{each secure link}}$), and the transmission powers that we will define in this section. The transmission power and receiving powers can be illustrated as in the following figure.

The powers we have defined in Section 2.1 are baseband transmit power P_t and based received power P_r, where the attenuation is due to baseband channel h (or small scale fading). The real transmission power and receiving power are defined as P_T and P_R, respectively, which are connected by propagation attenuation as

$$P_R = P_T K d^{-\alpha} \qquad (2.34)$$

where K is a constant, d is the propagation distance, and α is attenuation factor (normally within 2~4). After received the signal with power P_R, the receiver will amplify it, which we can describe as $P_t = AP_R$. Therefore, if we only consider small scale fading in a baseband channel model, then P_t is the modeled transmission power, not P_T.

A useful rule for us is that P_t and P_r are still linear with P_T, which means increasing the transmission power P_T by a factor also causes the increasing of P_t and P_r by the same factor.

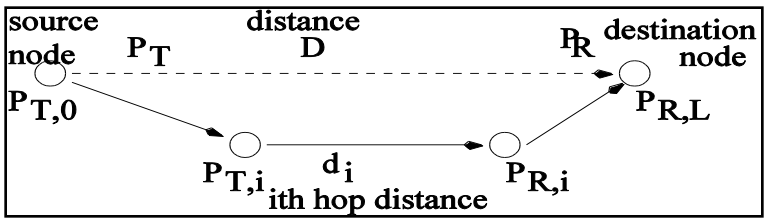

Figure 11 Multi-hop transmission/receiving powers compared to direct single-hop transmission/receiving powers.

2.2.1.1 A model for studying transmission power, transmission distance in multi-hop transmissions

We would like to study the transmission/receiving power of multi-hop data forwarding (with L hops). Instead of using absolute power (in terms of dBm), it is more convenient for us to model the transmission power as a comparison with the direct 1-hop transmission from the source to the destination.

Let the distance between the source node and the destination node be D meters. We may use a direct 1-hop transmission from the source node to the destination node, or we may employ relay nodes in the middle to form an L hop packet forwarding. Let us assume that each node needs to have a received signal power P_R in order to detect the signal successfully.

For the direct 1-hop transmission, the transmission power follows

$$P_R = P_{T,D} K D^{-\alpha}, \tag{2.35}$$

and the total transmission power in this case is just $P_{T,D}$.

Now let use consider the i^{th} hop, for $i = 0, \cdots, L-1$, with transmission power $P_{T,i}$ and received signal power P_R. We have

$$P_R = P_{T,i} K d_i^{-\alpha}. \tag{2.36}$$

Then the transmission power of the i^{th} hop can be described by the transmission power $P_{T,D}$ as

$$P_{T,i} = P_{T,D} \left(\frac{d_i}{D} \right)^{\alpha}. \tag{2.37}$$

Total transmission power required for this L-hop relaying case is then

$$P_{T,L} = \sum_{i=0}^{L-1} P_{T,i} = \frac{P_{T,D}}{D^{\alpha}} \sum_{i=0}^{L-1} d_i^{\alpha}. \tag{2.38}$$

Note that the distances usually satisfy

$$\sum_{i=0}^{L-1} d_i \geq D. \tag{2.39}$$

Under this setting (with targeting received signal power P_R), we can then calculate the data rate (or transmission capacity) of the multi-hop link as

$$R_L = \log_2\left(1+\frac{P_R}{P_N}\right) \text{ (bits/sec)}, \tag{2.40}$$

where P_N is the noise power which can be assumed identical for all receivers. This data rate is derived when we do not take any other interference and small scale channel fading into consideration. In other words, the direct 1-hop transmission can use total transmission power $P_{T,D}$ to realize this data rate, while the L-hop transmission has to use total transmission power $P_{T,L}$.

As one of possible optimization problems for multi-hop data forwarding, we can look for the best hop count L and the optimal hop distances d_i, by using the available relay nodes, so that the total transmission power is the lowest. A dual optimization problem is to optimize L and d_i such that the data rate is optimal under a fixed total transmission power. My existing work on multi-hop relay is something similar to the latter, but I also take into consideration the mutual interference and cooperation among the relay nodes into consideration.

2.2.1.2 A possible security measure: total broadcasting area

In this subsection, we propose to use the broadcasting area as a possible security metric. The reason is that a transmission with longer distance or larger transmission power, can be heard by more nodes in a larger area, and thus increases its interception probability. More adversary nodes may be able to jam the signal. In addition, larger transmission power may potentially interfere more friendly nodes nearby. As a result, we need to confine the broadcasting area.

For the direct 1-hop transmission with distance D, if P_R is the minimum required receiving signal power even for adversary nodes, then the broadcasting area is

$$S_D = \pi D^2. \tag{2.41}$$

For the L-hop transmission (with single transmitters), each hop transmission has a broadcasting area of

$$S_i = \pi d_i^2. \tag{2.42}$$

Considering the overlaps of adjacent hops, we may approximate the total area as

$$S_L = \sum_{i=0}^{L-1}\frac{2}{3}S_i = \frac{2\pi}{3}\sum_{i=0}^{L-1} d_i^2. \tag{2.43}$$

2.2.2 The application of our secure transmission scheme in multi-hop transmission

In this subsection, we analyze the transmission power and distances of our secure transmission scheme when used in this multi-hop relay scenario. In Section 1, we have presented it in a 1-hop transmission scenario. In that case, compared with the conventional single-antenna transmission/receiving that uses transmission power P_t to achieve a receiving SNR γ, our secure transmission can use a transmission power $P_{t,\text{secure}} = (2J-1)P_t$ to get an SNR $J\gamma$. Considering the linearity between the transmission power and the receiving power (and SNR), this also means that our secure transmission needs a transmission power $P_{t,\text{secure}} = \frac{2J-1}{J}P_t$ to guarantee the SNR γ.

Now let us apply our secure transmission scheme in the L-hop transmission. Because the secure transmission power relationship is derived based on small-scale fading, while the L-hop power relationship is made on large-scale fading, we need to connect them together. In other words, we need to consider that the received power P_R in large scale fading is connected to the transmission power P_t in small scale fading by

$$P_t = AP_R \tag{2.44}$$

where A is the amplification ratio of the receivers' power amplifier.

As stated in the above subsection, we need a transmission power $P_{T,i}$ for a transmission distance d_i. Let us assume that such as transmission power $P_{T,i}$ can also guarantee the SNR γ when considering the small scale fading. In other words, with a transmission power $P_{T,i}$, we can have a baseband transmission power P_t. Then in order to guarantee a baseband transmission power $P_{t,\text{secure}}$, we need a transmission power

$$P_{T,i,\text{secure}} = \frac{2J-1}{J}P_{T,i} \tag{2.45}$$

Note that even with the larger transmission power, the valid transmission distance is still d_i (for a targeting received power $\frac{2J-1}{J}P_R$ and SNR γ). In addition, the total number of hops is still L.

The total transmission power in this case is

$$P_{T,L,\text{secure}} = J\sum_{i=0}^{L-1}P_{T,i,\text{secure}} = J\frac{2J-1}{J}\sum_{i=0}^{L-1}P_{T,i} = \frac{(2J-1)P_{T,D}}{D^\alpha}\sum_{i=0}^{L-1}d_i^\alpha \ . \tag{2.46}$$

Note that the first J multiplication factor is because each transmission has to be repeated by J time for each of the J clustered receivers to receive the signal.

The higher transmission power is expended completely for transmission security, not for transmission distance or data rate. However, it does change the interference range with respect to other nodes.

The transmission date rate, if consider only large scale fading, is

$$R_{L,\text{secure}} = \frac{1}{J}\log_2\left(1+\frac{P_R}{P_N}\right), \tag{2.47}$$

where the divider J is still due to repeated transmissions.

Now let us include also the security measure. We must note that is may not be possible for the adversaries to intercept our transmission due to our secure design. However, the adversaries may still detect the existence of the transmission, or jam the transmission. Therefore, to some extent, we may still use the total broadcasting area as a simple security measure.

If our secure transmission is used in this multi-hop transmission, then the increased transmission power brings a larger broadcasting area although the targeting transmission distance d_i is still the same as the above.

Recall that the power $P_{T,i}$ causes a broadcasting distance d_i following $P_R = P_{t,i} K d_i^{-\alpha}$. So the new transmission power $P_{T,i,\text{secure}} = \frac{2J-1}{J} P_{T,i}$ should have a broadcasting distance $d_{i,\text{secure}}$ according to

$$P_R = P_{t,i,\text{secure}} K d_{i,\text{secure}}^{-\alpha}. \tag{2.48}$$

Therefore, the new broadcasting distance should be

$$d_{i,\text{secure}} = d_i \left(\frac{2J-1}{J} \right)^{\alpha}. \tag{2.49}$$

The broadcasting area of the hop i can be derived as

$$S_{i,\text{secure}} = \pi d_{i,\text{secure}}^2 = \pi d_i^2 \left(\frac{2J-1}{J} \right)^{2\alpha}. \tag{2.50}$$

Then the total broadcasting area of this L-hop secure transmission is

$$S_{L,\text{secure}} = \sum_{i=0}^{L-1} \frac{2}{3} S_{i,\text{secure}} = \frac{2\pi}{3} \left(\frac{2J-1}{J} \right)^{2\alpha} \sum_{i=0}^{L-1} d_i^2. \tag{2.51}$$

For network optimization, we need to determine the hop count L, the cluster size J, and the hop distances d_i, so as to increase data rate R_L, reduce total transmission power $P_{T,L}$, or reduce total broadcasting area S_L.

In summary, for the conventional multi-hop transmission with single transmitter/receiver, we have the optimization problem

$$\text{Optimize } L, J, d_i, \text{ for } i = 0, \cdots, L-1, \text{ so as to}$$

$$\begin{cases} \max \quad R_L = \log_2 \left(1 + \dfrac{P_R}{P_N} \right) \\ \min \quad P_{T,L} = \dfrac{P_{T,D}}{D^{\alpha}} \displaystyle\sum_{i=0}^{L-1} d_i^{\alpha} \\ \min \quad S_L = \dfrac{2\pi}{3} \displaystyle\sum_{i=0}^{L-1} d_i^2 \end{cases} . \tag{2.52}$$

$$\text{s.t., } L = 1, 2, \cdots; \quad J = 1, 2, \cdots; \quad \sum_{i=0}^{L-1} d_i \geq D; \quad d_i > 1.$$

For our secure transmission (or the clustering case), we have the optimization problem

$$\text{Optimize } L, J, d_i, \text{ for } i = 0, \cdots, L-1, \text{ so as to}$$

$$\begin{cases} \max \quad R_{L,\text{secure}} = \dfrac{1}{J}\log_2\left(1+\dfrac{P_R}{P_N}\right) \\ \min \quad P_{T,L,\text{secure}} = \dfrac{(2J-1)P_{T,D}}{D^\alpha}\displaystyle\sum_{i=0}^{L-1} d_i^\alpha \\ \min \quad S_{L,\text{secure}} = \dfrac{2\pi}{3}\left(\dfrac{2J-1}{J}\right)^{2\alpha}\displaystyle\sum_{i=0}^{L-1} d_i^2 \end{cases} . \tag{2.53}$$

$$\text{s.t., } L = 1,2,\cdots; \quad J = 1,2,\cdots; \quad \sum_{i=0}^{L-1} d_i \geq D \quad d_i > 1.$$

Note that the former is a special case of the latter when $J = 1$ (unclustering). In particular, when optimizing the data rate R_L, we may just need to assume certain P_R, P_N (large scale fading case), or single-antenna transmission rate R values as basic unit.

Note that we have the constraint $d_i > 1$ because otherwise, we may get unrealistic results $P_R > P_T$.

2.2.3 The application of beamforming scheme in multi-hop transmissions

When applying the beamforming scheme in multi-hop transmissions, the related performance evaluation rule can be derived similarly as Section 2.4. We assume that the receiver require baseband (when considering small-scale fading only) SNR γ and require passband (when considering large-scale fading only) received power P_R in order to work, for both single transmitter case and beamforming case.

Let us consider first the transmission power. From Section 2.3, we know that in order to guarantee SNR γ similarly as single-transmitter case, the J transmitter beamforming scheme just needs a transmission power of P_t/J, which also means that P_R/J and P_T/J can be used. With such a reduced total transmission power, however, the valid transmission distance d_i in each hop does not change. Specifically, if in single-transmitter multi-hop case, the i^{th}-hop needs transmission power $P_{T,i} = P_{T,D}\left(\dfrac{d_i}{D}\right)^\alpha$ to reach the transmission distance d_i, then in beamforming case, the reduced transmission power

$$P_{T,i,\text{beamform}} = \frac{P_{T,i}}{J} \tag{2.54}$$

can still guarantee the valid transmission distance d_j. This means that beamforming can save transmission power. An alternative explanation is that if we fix the transmission power, then beamforming can guarantee a longer transmission distance with targeting received signal power P_R/J and SNR γ. We use the former description because it more directly relates to our security criteria.

The total transmission power is

$$P_{T.\text{beamform}} = \sum_{i=0}^{L-1} P_{T,i,\text{beamform}} = \frac{P_{T,D}}{JD^\alpha}\sum_{i=0}^{L-1} d_i^\alpha \tag{2.55}$$

The transmission data rate does not change in this setting, i.e.,

$$R_{L,\text{beamform}} = \log_2(1+\gamma). \tag{2.56}$$

To eavesdroppers, the coverage area of this multi-hop beamforming scheme is smaller than that of the desirable user, because the SNR of eavesdropper is smaller than the SNR of the desirable user by a factor J. The baseband model will give the eavesdropper with an SNR

$$\gamma_e = \frac{\gamma}{J}. \tag{2.57}$$

This reduction of baseband SNR must be compensated by the reduction of the valid receiving distance to

$$d_{e,i} = J^{-\frac{1}{\alpha}} d_i. \tag{2.58}$$

Considering that each hop has a listening area

$$S_{e,i} = \pi d_{e,i}^2 \tag{2.59}$$

we can approximate the total listening area as

$$S_e = \sum_{i=0}^{L-1} \frac{2}{3} S_{e,i} = \frac{2\pi}{3} J^{-\frac{2}{\alpha}} \sum_{i=0}^{L-1} d_i^2. \tag{2.60}$$

Note that the factor $2/3$ is added in consideration of the overlap between adjacent hops.

In summary, for multi-hop beamforming scheme, we can have the following optimization problem to look for optimal hop number L, cluster size J, and hop distances d_i,

$$\text{Optimize } L, J, d_i, \text{ for } i = 0, \cdots, L-1, \text{ so as to}$$

$$\begin{cases} \max \quad R_{L,\text{beamform}} = \log_2(1+\gamma) \\ \min \quad P_{T,\text{beamform}} = \dfrac{P_{T,D}}{JD^{\alpha}} \displaystyle\sum_{i=0}^{L-1} d_i^{\alpha} \\ \min \quad S_e = \dfrac{2\pi}{3} J^{-\frac{2}{\alpha}} \displaystyle\sum_{i=0}^{L-1} d_i^2 \end{cases}. \tag{2.61}$$

$$\text{s.t., } L = 1, 2, \cdots; \quad J = 1, 2, \cdots; \quad \sum_{i=0}^{L-1} d_i \geq D \quad d_i > 1.$$

The optimization does look that larger J is always better in the beamforming case. The cost paid for larger J is the synchronization and coordination of larger clusters, which is not taken into consideration in our formulation. However, when *J* is constrained by the total number of agents, i.e., the larger the *J*, the smaller the *L*, the outcome of this optimization is the same as that resulted from (2.20) the new secure transmission configuration. Figure 14 shows the simulation results from a 100-node network with beam-forming.

2.2.4 Another possible optimization framework

In this section, we try to propose an overall optimization function, which optimizes parameters $L, J, d_i, P_{T,D}$ for lower energy consumption and lower ratio of (adversaries') listening area and (authorized users') sensing area. Specifically, we try to include the concept of sensing area into our optimization framework.

We have seen in previous sections that using J-node clustered transmissions, we can reduce the adversaries' listening distance from d_i (which is the authorized target's receiving distance) to $d_{e,i} = J^{-1/\alpha} d_i$. This means that larger cluster is better for security.

If we consider the sensing range of the cluster, where each node of the cluster may be a sensor, and we may assume that the cluster may conduct certain joint processing to extract the sensed information. According to the beamforming theory, the J -node cluster will provide a J -fold increase of sensing SNR. As a result, the valid sensing range becomes as larger as

$$d_{s,i} = J^{\frac{1}{\alpha}} d_i . \tag{2.62}$$

The sensing coverage, or the sensing area, of the i^{th} cluster is thus

$$S_{s,i} = \pi d_{s,i}^2 , \tag{2.63}$$

and the total sensing area is

$$S_s = \sum_{i=0}^{L-1} \frac{2}{3} S_{s,i} = \frac{2\pi}{3} J^{\frac{2}{\alpha}} \sum_{i=0}^{L-1} d_i^2 . \tag{2.64}$$

This equation leads to the conclusion that large cluster size is also better for increasing sensing coverage.

Instead of considering many different optimization objectives, we may just consider two of them. The first is the overall energy consumed, which equals to the transmission power times the transmission duration, and we can simply use the transmission power divided by the transmission data rate as the energy criteria.

For this purpose, we first need to parameterize the transmission data rate, or the SNR equation. Our deductions in the previous sections are all based on the assumption that the overall SNR is identical between the 1-hop direct transmission and the multi-hop transmissions with or without beamforming. In this case, the SNR can be described by

$$\gamma = C P_{T,D} D^{-\alpha} . \tag{2.65}$$

Then the energy consumption is described by

$$E_{beamform} = \frac{P_{T,beamform}}{R_{L,beamform}} = \frac{\frac{P_{T,D}}{JD^{\alpha}} \sum_{i=0}^{L-1} d_i^{\alpha}}{\log_2(1 + C P_{T,D} D^{-\alpha})} . \tag{2.66}$$

As to the second criteria, we use the ratio between the listening area and the sensing area,

$$A_{beamform} = \frac{S_e}{S_s} = \frac{\frac{2\pi}{3} J^{-\frac{2}{\alpha}} \sum_{i=0}^{L-1} d_i^2}{\frac{2\pi}{3} J^{\frac{2}{\alpha}} \sum_{i=0}^{L-1} d_i^2} = J^{-\frac{4}{\alpha}} . \tag{2.67}$$

Then the overall optimization criteria is to minimize both $E_{beamform}$ and $A_{beamform}$, which becomes

$$\min \quad F(L, J, d_i, P_{T,D}) = \beta_1 E_{beamform} + \beta_2 A_{beamform} \tag{2.68}$$

under constraints

$$\begin{cases} L = 1, 2, \cdots, \min(D, M), \\ J = 1, 2, \cdots, \dfrac{M}{L} \\ \displaystyle\sum_{i=0}^{L-1} d_i \geq D \\ d_i > 1, \quad i = 0, \cdots, L-1 \\ P_{T,D} > 0 \end{cases} \tag{2.69}$$

Note that M is total number of nodes available.

2.2.5 Channel failure probability

Network reliability studies require the channel failure probability model. In this subsection, we derive the channel failure probability as an outage probability, which is defined as the received signal's power is less than a power threshold and thus causes the loss of transmitted signal. We assume that the underline reason of this channel failure is the random channel fading, from which we can derive the explicit expression of the channel failure probability as an exponential function of the propagation distance.

Let the transmit power be P_T, and transmission distance be d. Trom the large-scale propagation attenuation, the received signal power is $P_R = P_T K d^{-\alpha}$, where K and α are a constant and the signal attenuation exponential factor.

Now we need to consider the small scale fading. Let the receiver has a power amplification ratio A. Then purely from the small scale fading model, we can model the transmission power as $P_t = AP_R = AKP_T d^{-\alpha}$. Let the small scale fading channel be h, which is a complex Gaussian random variable with zero mean and unit variance. Then the received signal's power is

$$P_r = P_t \mid h \mid^2 = AKP_T d^{-\alpha} \left|h\right|^2 . \tag{2.70}$$

We define the channel failure as an outage probability,

$$P[P_r < P_0] \tag{2.71}$$

which denotes that the received signal's power is less than a power threshold P_0. Then we have

$$P[P_r < P_0] = P\left[\left|h\right|^2 < \frac{P_0}{AKP_T} d^{\alpha}\right]. \tag{2.72}$$

Because $\left|h\right|^2$ is an exponential random variable with unit mean, the above probability can be evaluated as

$$P[P_r < P_0] = \int_0^{\frac{P_0}{AKP_T} d^{\alpha}} e^{-x} dx = 1 - e^{-\frac{P_0}{AKP_T} d^{\alpha}} , \tag{2.73}$$

which shows that the channel failure probability is an exponential function of the propagation distance d (more exactly, d^{α}).

2.3 A numerical example

In this section, we use a numerical example to demonstrate the multi-hop wireless network optimization problem. Considering that we are more concerned about the transmission data rate than the transmission power, we put transmission power as a constraint while optimizing transmission data rate and the adversary's listening area.

Before we go into simulation details, the observation of the numerical evaluation is summarized as follows

- For *non-clustered* multi-hop transmissions, if we fix the transmission power of each node, then more nodes and thus more hops are always better for enhancing data rate, but are always worse for reducing listening area. As a result, there is an optimal hop or node account that can optimize both data rate and listening area.
- For clustered multi-hop transmissions, if we fix the total number of nodes and the transmission power of each node, then smaller cluster size and more hops are always better for both enhancing data rate and reducing listening area. This means that the optimization always favors *non-clustered* multi-hop transmission that uses all available nodes as relays.

The simulation parameters are as follows:

- Constant $K = 6.3\times10^{-5}$, which is calculated from a carrier frequency 3 GHz, unit antenna gains, with equation $K = G_t G_r \lambda^2 / (4\pi)^2$;
- A fixed transmission power $P_T = 20$ watts for each node, which does not change even in clustered transmissions;
- Overall transmission distance $D = 50$ km, which denotes the distance from the source to the destination;
- Propagation attenuation exponential factor $\alpha = 3$;
- A fixed noise power for each node $P_N = -110$ dBm;
- A power threshold $P_0 = -90$ dBm for listening, which also means a required SNR 20 dB for successful listening and receiving at data rate $R = 6.66$ bps/Hz.
- Total number of nodes in the network is $M = 100$, which includes one source, one destination, and 98 relaying nodes.

Let us first see the direct transmission from the source to the destination without any relaying. The received power is

$$P_R = P_T K D^{-\alpha} = 10^{-14} = -139 \text{ dBm}. \tag{2.74}$$

which gives an SNR of -29 dB. This SNR does not satisfy the listening/receiving requirement, although theoretically the transmitter may use some special coding scheme such as spread spectrum to achieve a date rate of $R_0 = \log_2(1+10^{-29/10}) = 0.0018$ bps/Hz.

The adversary's effective listening distance in this case can be calculated from $P_0 = P_T K d_0^{-\alpha}$, which gives $d_0 = 1.1$ km. So the listening area is $A_0 = \pi d_0^2 = 3.8$ square km.

2.3.1 Non-clustered multi-hop relaying

If we use some or all of the relaying nodes, e.g., we use $m-2$ relaying nodes to form an $m-1$ hop relay network, where $2 \le m \le M$. Since we have assumed that all the nodes have identical transmission power, the distance of each hop should also be identical for optimality. Therefore, the hop distance is

$$d_i = \frac{D}{m-1}, \qquad i = 0, \cdots, m-2, \tag{2.75}$$

The received signal power of each hop node is

$$P_{R,i} = P_T K d_i^{\alpha} = (m-1)^3 \times 10^{-14}. \tag{2.76}$$

The SNR is thus $\left(\frac{m-1}{10}\right)^3$. In order to satisfy the SNR constraint, we need $\left(\frac{m-1}{10}\right)^3 \ge 10^{\frac{20}{10}}$, which gives $m \ge 48$. In other words, we need to use a total of at least 48 nodes to form 47 or more hops in order to satisfy this SNR requirement. Nevertheless, the data rate of any m node relaying transmission path can be calculated as

$$R_m = \log_2\left[1+\left(\frac{m-1}{10}\right)^3\right], \tag{2.77}$$

which shows a monotone increasing of data rate when more relaying nodes are used. The highest available data rate is $R_{100} = 9.92$ bps/Hz when all the $M = 100$ nodes are used and are placed in the optimal position (i.e., with an equal hop distance $d_i = 50/(100-1) = 0.5051$ km).

For the adversary's listening area, since the node transmission power is fixed, so the listening distance of each hop is still $d_0 = 1.1$ km. Therefore, the total listening area is approximately $A_m = \pi d_0^2 (m-1) = 3.8(m-1)$ square km. The more relaying hops are involved, the larger listening area.

If we want to maximize data rate while to minimize listening area according to the following objective:

$$\max f(m) = \frac{R_m}{R_M} - \frac{A_m}{A_M} = 0.1 \times \log_2 \left[1 + \left(\frac{m-1}{10} \right)^3 \right] - 0.003 \times 3.8(m-1), \; m = 2, \cdots, 100. \quad (2.78)$$

Note that we have to normalized R_m and A_m because of their big difference in values. The curve of $f(m)$ as a function of m is show in the figure below. Then the optimal solution is $m = 38$ and $f(m) = f(38) = 0.1473$. Note that even in this case, the received signal's SNR is about 17 dB, still below the targeting SNR 20 dB, and the data rate is 5.69 bps/Hz.

2.3.1.1 Multi-hop relay on a circle

Instead of considering multi-hop relays in a straight-line, we may also be interested in considering the coverage of some other area shapes. In particular, we may consider the targeting coverage area as a circle. Let the total transmission distance still be D, and we need at least two nodes which forms at least two hops from the source to the source.

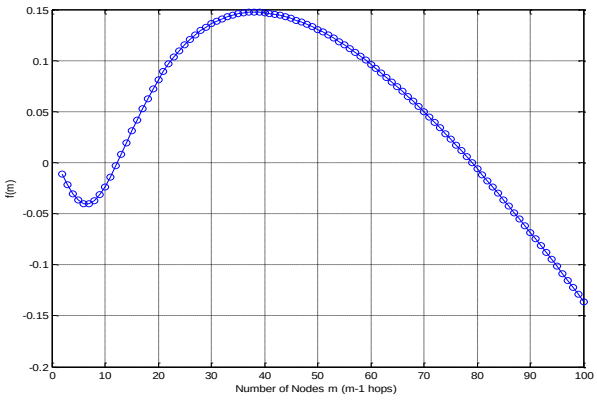

Figure 12 Optimization for multi-hop wireless transmission network with non-clustered transmissions.

When we use m nodes to form an m hop from the source to the source, then each node will have a transmission distance $d_i = D/m$. Note that instead of the circumference of a circle, we actually assume the total direct-line propagation distance is D. Then similarly as the straight-line case, the received power of each node is $P_{R,i} = P_T K D^{-3} m^3 = m^3 \times 10^{-14}$, which gives SNR $(m/10)^3$ and data rate $R_m = \log_2 \left[1 + (m/10)^3 \right]$. The listerning area can be similarly found as $A_m = \pi d_0^2 m = 3.8m$. Therefore, the optimization problem is almost identical to the straight-line case.

Because of such similarity, we only consider the straight-line case in the following clustered transmission studies.

2.3.2 Multi-hop relaying with clustered beamforming

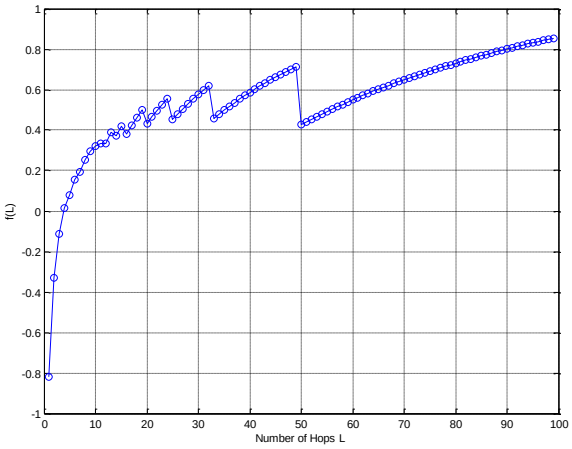

Figure 13 Optimization for multi-hop wireless transmission network with beamforming.

To simplify the problem, we fix the total number of available nodes to $M = 100$. Let the hop account be L, which means we have $L+1$ clusters (including the source cluster and the destination cluster) and each cluster has $J = \lfloor M/(L+1) \rfloor$ nodes. The transmission distance of each hop is $d_i = D/L$.

Since each node has a transmission power P_T, the total transmission power of each cluster is thus JP_T. If conventional beamforming scheme is used, such a total transmission power will cause a total received signal power $P_{R,i} = JP_T K d_i^{-\alpha}$. Considering that each receive node now has J copies of the same signal, the small-scaling fading effect will contribute another J-fold increase of SNR. Specifically, the received signal power in the baseband small-scale fading model is

$$P_{r,i} = AP_{R,i} E\left\{\sum_{j=1}^{J} |h_{j,i}|^2\right\} = JAP_{R,i} = J^2 AP_T K d_i^{-\alpha} \tag{2.79}$$

which gives a J^2-fold increase of the SNR to

$$\gamma_{beamform}(L) = J\frac{P_{R,i}}{P_N} = J^2 \frac{P_T K D^{-\alpha}}{P_N} L^{\alpha} = J^2 L^3 10^{-3}. \tag{2.80}$$

The transmission data rate in this case is thus

$$R_{beamform}(L) = \log_2(1+\gamma_{beamform}(L)) = \log_2(1+J^2 L^3 10^{-3}). \tag{2.81}$$

For the special cases that $J \approx M/L$, we can reduce the above equation to $R_{beamform}(L) \approx \log_2(1+M^2 L 10^{-3}) = \log_2(1+M^3 J^{-1} 10^{-3})$, from which we can see that the data rate increases with more hops and smaller cluster size. In particular, the highest data rate is achieved when using 99 hops and one-node per cluster (non-clustered transmission). Such a highest data rate equals to R_{100} derived in Section 2.2.4.

Now let us consider the adversary's listening area. According to the derivation in Section 2.2, the listening distance is

$$d_{e,i} = J^{-\frac{1}{\alpha}} d_i = J^{-\frac{1}{\alpha}} \frac{D}{L}. \tag{2.82}$$

Therefore, the total listening area can be approximated as

$$A_{beamform} = \frac{2}{3}\sum_{i=0}^{L-1}\pi d_{e,i}^2 = \frac{2}{3}L\pi\left(J^{-\frac{1}{\alpha}}\frac{D}{L}\right)^2 = \frac{2}{3}\pi D^2 J^{-\frac{2}{3}}L^{-1}. \quad (2.83)$$

For the special cases that $J \approx M/L$, we can simplify the above equation to $A_{beamform} \approx \frac{2}{3}\pi D^2 J^{\frac{1}{3}}M^{-1} = \frac{2}{3}\pi D^2 L^{-\frac{1}{3}}M^{-\frac{2}{3}}$, from which we can readily see that smaller listening area also prefers larger number of hops with smaller cluster size. In particular, the conventional single-node cluster (non-cluster) $M-1$ hop transmission gives the optimal result.

From both the transmission rate and listening area results, we have seen that smaller cluster size and more hops are always better, if we have a fixed number of nodes to use. This conclusion can be demonstrated numerically be maximizing

$$\begin{aligned}\max f(L) &= \frac{R_{beamform}(L)}{R_{beamform}(M-1)} - \frac{A_{beamform}(L)}{A_{beamform}(1)} \\ &= 0.1\times\log_2(1+J^2L^3 10^{-3}) - 13.57\times J^{-\frac{2}{3}}L^{-1} \quad (2.84)\\ s.t.,\ J &= \left\lfloor \frac{100}{L+1} \right\rfloor, \qquad L = 1,\cdots,99.\end{aligned}$$

The numerical evaluation of $f(L)$ is show in the following figure, which clearly indicates the favor of larger number of hops (and thus smaller cluster sizes). Note that the saw-tooth structure is due to the fact the some of the 100 nodes may not be used for many hop accounts.

2.3.3 Multi-hop relaying with clustered secure transmission

Instead of beamforming, we may consider asking each cluster to implement our secure transmission scheme to enhance transmission security. In this new transmission scheme, each cluster will have to use $(2J-1)$-fold of total transmission power as the conventional single-node transmission, and the receiver will have a J-fold increase of SNR compared with the latter. Note that on average, each node in the cluster will have $(2J-1)/J \approx 2$ fold of the single-node transmission power.

For fair comparison, we will divide the total transmission power by a factor $(2J-1)/J$ so as to ach node in the cluster still use the fixed transmission power P_T. In other words, the total transmission power of each cluster is still JP_T, just as the conventional beamforming. Then the receiver will see an SNR

$$\gamma_{\text{secure}}(L) = J\frac{P_T K}{P_N}\left(\frac{D}{L}\right)^{-\alpha}\frac{J}{2J-1} = \frac{J^2}{2J-1}L^3 10^{-3}. \quad (2.85)$$

With such an SNR, the transmission data rate is

$$R_{\text{secure}}(L) = \frac{1}{J}\log_2(1+\gamma_{\text{secure}}(L)) = \frac{1}{J}\log_2\left(1+\frac{J^2}{2J-1}L^3 10^{-3}\right). \quad (2.86)$$

For the special cases that $J \approx M/L$, we can reduce the above equation to $R_{\text{secure}}(L) \approx \frac{1}{J}\log_2\left(1+\frac{M^3}{J(2J-1)}10^{-3}\right)$, which also indicates smaller cluster size is better for enhancing transmission data rate.

As to the adversary's listening area, we have the listening distance $d_{e,i} = d_i\left((2J-1)/J\right)^{\alpha}$. Therefore, the total listening area is

$$A_{\text{secure}}(L) = \frac{2}{3}\sum_{i=0}^{L-1}\pi d_{e,i}^2 = \frac{2}{3}L\pi\left(\frac{D}{L}\right)^2\left(\frac{2J-1}{J}\right)^{2\alpha} = \frac{2}{3}\pi D^2 L^{-1}\left(\frac{2J-1}{J}\right)^6. \qquad (2.87)$$

For the special cases that $J \approx M/L$, we can simplify the above equation to $A_{\text{secure}}(L) \approx \frac{2}{3}\pi D^2 M^{-1}\frac{(2J-1)^6}{J^5} \approx \frac{2}{3}\pi D^2 M^{-1} 2^6 (2J-1)$, which also prefers smaller cluster size J for reducing listening area.

From both the transmission rate and listening area results, we still see that smaller cluster size and more hops are always better, if we have a fixed number of nodes to use. This conclusion can also be demonstrated numerically be maximizing

$$\begin{aligned}\max f(L) &= \frac{R_{\text{secure}}(L)}{R_{\text{secure}}(M-1)} - \frac{A_{\text{secure}}(L)}{A_{\text{secure}}(1)} \\ &= 0.1\times\frac{1}{J}\log_2\left(1+\frac{J^2L^3 10^{-3}}{2J-1}\right) - 0.017\times L^{-1}\left(\frac{2J-1}{J}\right)^6 \qquad (2.88)\\ \text{s.t.,}\ \ J &= \left\lfloor\frac{100}{L+1}\right\rfloor, \qquad L = 1,\cdots,99.\end{aligned}$$

The numerical evaluation of $f(L)$ is show in the following figure, which clearly indicates the favor of larger number of hops (and thus smaller cluster sizes). Note that the saw-tooth structure is due to the fact the some of the 100 nodes may not be used for many hop accounts.

2.3.4 Network reliability

Network reliability is now considered to set bounds for the above optimization problem. As an initial attempt, channels are assumed to be perfect, and only node failures are considered. A lower bound of a multiple hop network reliability was derived in [8]. With assumed high channel reliability, the lower bound becomes exact and is given by

$$\prod_{i=1}^{L} \underline{R}_i^J, \quad \underline{R}_i^J = \sum_{s=k}^{J} \binom{J}{s} r^s (1-r)^{J-s} \qquad , \; J \times L = N \tag{2.89}$$

where r is the node reliability. The number of nodes J in a cluster is constrained by $floor(N / L)$, where N is the total number of airborne nodes and L is the number of clusters in the network.

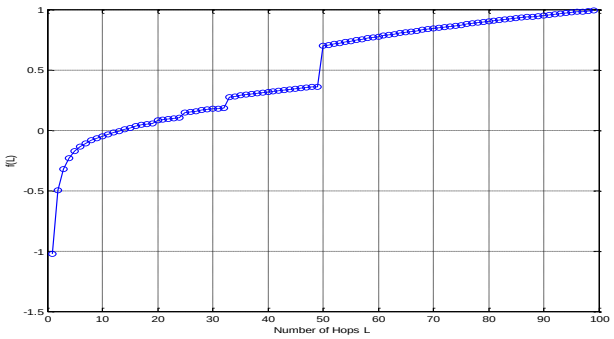

Figure 14 Optimization for multi-hop wireless transmission network with clustered secure transmissions.

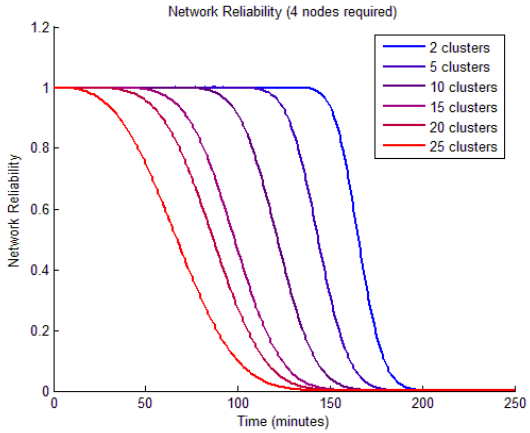

Figure 15 Network reliability as a function of time with cluster number as a parameter (Weibull node failure probability assumed, and minimum of 4 surviving agents required for an operative cluster)

It can be seen that network reliability increases with increasing number of agents in a cluster when the total number agents is constrained at 100. In combination with the results of optimization that consider only security, power, and data rate, overall optimal clustering is to divide the 100 nodes into 25 clusters of 4-agent each.

3. Conclusions

In this report, we show our progress during the first summer of the project. We have successfully set up single-link and multi-hop wireless transmission models, for single node transmissions, clustered cooperative secure transmissions, and clustered cooperative beamforming transmissions. Based on such transmission models, multiple objective optimization frameworks for optimizing multi-hop wireless networking parameters are proposed. The objectives include transmission efficiency metrics such as SINR and data rate, network reliability metrics such as network lifetime, and network security metrics such as eavesdropper's listening area. The optimization parameters include the cluster size, hop account, hop distances, etc. Some preliminary analysis and simulations have been conducted, which indicates that such optimization is meaningful and necessary. This summer's work provides us with solid background for the subsequence work of this research.

For the continuing work, an immediate task is to taken node competition into consideration, besides node cooperation for clustering and multi-hop data forwarding. This task is in fact in our work immediately after this summer. Node competition is quantified by the mutual interference among clusters. For the conventional single node multi-hop transmission, the SINR of each hop is derived, and this indicates a complex inter-connection among the transmissions of each hop. We are working on including clustered cooperative transmission into this scheme, and set up the optimization framework in order to compare the various networking parameters [26,27].

Another task, as outline as the proposed second summer's work, we will focus on deriving a general network structure function to capture all aspects of expectations, under which a tasking policy is solved through, for example, a Markov decision process. More specifically, distributed optimization problem for cooperative transmissions and mode switching policy will be formulated and solved simultaneously. The general method of multi-hop network capacity and performance analysis will be extended to considering nodes or link reliability. We will develop efficient ways to evaluate the network reliability for multi-hop wireless networks under nodes cooperation and competition, which will then be integrated into the distributed optimization problem. In addition, a quantifiable notion of security will be defined, and the interplay between redundancy and security will be examined.

4. References

[1] P. Antsaklis, "Special issue on hybrid systems: theory and applications a brief introduction to the theory and applications of hybrid systems," *Proceedings of the IEEE*, vol. 88, no. 7, pp. 879–887, 2000.

[2] A. Bemporad and M. Morari, "Robust model predictive control: A survey," *Robustness in Identification and Control*, vol. 245, pp. 207–226, 1999.

[3] D. Bertsekas, *Nonlinear programming*. Athena Scientific Belmont, Mass, 1999.

[4] T. Busch, "Modeling of air operations for course-of-action determination," *Proceedings of SPIE*, vol. 4716, p. 35, 2002.

[5] P. Campo and M. Morari, "Robust model predictive control," *Proceedings of the 1987 American Control Conference*, vol. 2, pp. 1021–1026, 1987.

[6] G. Casella, R. Berger, and R. Berger, *Statistical inference*. Duxbury Press Belmont, Calif, 1990.

[7] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, 1999.

[8] J. Jelinek, "Models for computing combat risk," *Proceedings of SPIE*, vol. 4716, p. 52, 2002.

[9] E. Kao, *An introduction to stochastic processes*. Duxbury Press, 1997.

[10] H. Khalil, *Nonlinear systems*. Prentice Hall Upper Saddle River, NJ, 1996.

[11] W. Kwon and S. Han, *Receding Horizon Control: Model Predictive Control for State Models*. Springer, 2005.

[12] Mathworks, Matlab. Natick, MA: Mathworks, Inc., 2008.

[13] ——, Optimization Toolbox. Natick, MA: Mathworks, Inc., 2008.

[14] ——, SimEvents Toolbox. Natick, MA: Mathworks, Inc., 2008.

[15] ——, Simulink. Natick, MA: Mathworks, Inc., 2008.

[16] J. Rawlings, "Tutorial overview of model predictive control," *Control Systems Magazine*, IEEE, vol. 20, no. 3, pp. 38–52, 2000.

[17] M. Ruschmann, "Receding horizon control of air operation resource allocation," Master's thesis, Binghamton University, 2006.

[18] J. Wohletz, D. Castanon, M. Curry, A. Inc, and M. Burlington, "Closed-loop control for joint air operations," *American Control Conference, 2001. Proceedings of the 2001*, vol. 6, 2001.

[19] N. Wu and T. Busch, "Strategic reconfigurability in air operations," *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, vol. 6, 2003.

[20] N. Wu and M. Ruschmann, "Loop Closure for Enhanced Win Percentage in an Air Operation," *American Control Conference, 2007. ACC'07*, pp. 1097–1102, 2007.

[21] P. Antsaklis and J. Baillieul, editors, Special issue on Technology of Networked Control Systems, *Proceedings of the IEEE*, vol.95, Issue 1, 2007.

[22] M. D. Bailey, M. Tavana, and T. E. Busch, "Communication Role Allocation for Joint Air Operations in a Network-Centric Environment," *International Journal of Computer Science and Network Security*, Vol.6, No.12, pp.165-170, 2006.

[23] X. Li, J. Hwu and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24-32, May 2007.

[24] D. H. Johnson and D. E. Dudgeon, *Array Signal Processing: Concepts and Techniques*, Prentice Hall PTR, 1993.

[25] J. Proakis, *Digital Communications*, 4th Ed. New York: McGraw-Hill, 2000.

[26] X. Li, J. Hwu and F. Ng, "Transmission power and capacity of secondary users in a dynamic spectrum access network," *IEEE Military Communications Conference* (MILCOM'2007), Orlando, FL, Oct. 29-31, 2007

[27] X. Li, “Efficient algorithm for hop optimization in multi-hop ad hoc wireless networks,” *Proceedings of 2008 ICST Second International Conference on Networks for Grid Applications and Workshops -- Wireless Grids,* Beijing, China, Oct. 8-10, 2008.

[28] N.E.Wu, S. Thavamani, and X. Li, Reliability and Feedback of Multiple Hop Wireless Networks, *International Journal of Automation and Computing*, vol. 4, pp.125-134, 2007.